H3C MSR 20/30/50 Series Routers
Command Reference Manual (v1.00)

MSR 20 Series Routers
MSR 30 Series Routers
MSR 50 Series Routers

www.3Com.com
Part Number: 10016323 Rev. AA
August 2007

3Com Corporation
350 Campus Drive
Marlborough, MA
USA 01752-3064

3Com Corporation reserves the right to revise this documentation and to make changes in content from time to time without obligation on the part of 3Com Corporation to provide notification of such revision or change.

3Com Corporation provides this documentation without warranty, term, or condition of any kind, either implied or expressed, including, but not limited to, the implied warranties, terms or conditions of merchantability, satisfactory quality, and fitness for a particular purpose. 3Com may make improvements or changes in the product(s) and/or the program(s) described in this documentation at any time.

If there is any software on removable media described in this documentation, it is furnished under a license agreement included with the product as a separate document, in the hard copy documentation, or on the removable media in a directory file named LICENSE.TXT or !LICENSE.TXT. If you are unable to locate a copy, please contact 3Com and a copy will be provided to you.

UNITED STATES GOVERNMENT LEGEND

If you are a United States government agency, then this documentation and the software described herein are provided to you subject to the following:

All technical data and computer software are commercial in nature and developed solely at private expense. Software is delivered as "Commercial Computer Software" as defined in DFARS 252.227-7014 (June 1995) or as a "commercial item" as defined in FAR 2.101(a) and as such is provided with only such rights as are provided in 3Com's standard commercial license for the Software. Technical data is provided with limited rights only as provided in DFAR 252.227-7015 (Nov 1995) or FAR 52.227-14 (June 1987), whichever is applicable. You agree not to remove or deface any portion of any legend provided on any licensed program or documentation contained in, or delivered to you in conjunction with, this User Guide.

Unless otherwise indicated, 3Com registered trademarks are registered in the United States and may or may not be registered in other countries.

3Com and the 3Com logo are registered trademarks of 3Com Corporation.

H3C, , Aolynk, , H3Care, , TOP G, , IRF, NetPilot, Neocean, NeoVTL, SecPro, SecPoint, SecEngine, SecPath, Comware, Secware, Storware, NQA, VVG, V2G, VnG, PSPT, XGbus, N-Bus, TiGem, InnoVision and HUASAN are trademarks of Hangzhou H3C Technologies Co., Ltd., a 3Com company.

All other trademarks that may be mentioned in this manual are the property of their respective owners.

ENVIRONMENTAL STATEMENT

It is the policy of 3Com Corporation to be environmentally-friendly in all operations. To uphold our policy, we are committed to:

Establishing environmental performance standards that comply with national legislation and regulations.

Conserving energy, materials and natural resources in all operations.

Reducing the waste generated by all operations. Ensuring that all waste conforms to recognized environmental standards. Maximizing the recyclable and reusable content of all products.

Ensuring that all products can be recycled, reused and disposed of safely.

Ensuring that all products are labelled according to recognized environmental standards.

Improving our environmental record on a continual basis.

End of Life Statement

3Com processes allow for the recovery, reclamation and safe disposal of all end-of-life electronic components.

Regulated Materials Statement

3Com products do not contain any hazardous or ozone-depleting material.

Environmental Statement about the Documentation

The documentation for this product is printed on paper that comes from sustainable, managed forests; it is fully biodegradable and recyclable, and is completely chlorine-free. The varnish is environmentally-friendly, and the inks are vegetable-based with a low heavy-metal content.

CONTENTS

6 ADSL INTERFACE CONFIGURATION COMMANDS

7 POS INTERFACE CONFIGURATION COMMANDS

8 GENERAL ETHERNET INTERFACE CONFIGURATION COMMANDS

9 CONFIGURATION COMMANDS FOR ETHERNET INTERFACES IN BRIDGE MODE

10 CONFIGURATION COMMANDS FOR ETHERNET INTERFACES IN ROUTE MODE

11 FUNDAMENTAL SERIAL INTERFACE CONFIGURATION COMMANDS

12 FUNDAMENTAL CE1/PRI INTERFACE CONFIGURATION COMMANDS

15 T1-F INTERFACE CONFIGURATION COMMANDS

16 FUNDAMENTAL CE3 INTERFACE CONFIGURATION COMMANDS

17 FUNDAMENTAL CT3 INTERFACE CONFIGURATION COMMANDS

21 BASIC DLSW CONFIGURATION COMMANDS

22 FRAME RELAY CONFIGURATION COMMANDS

27 LINK AGGREGATION CONFIGURATION COMMANDS

28 LINK AGGREGATION DEBUGGING COMMANDS

29 MODEM CONFIGURATION COMMANDS

30 PORT MIRRORING CONFIGURATION COMMANDS

31 PPP AND MP CONFIGURATION COMMANDS

35 PPP DEBUGGING COMMANDS

36 BRIDGING CONFIGURATION COMMANDS

37 ISDN CONFIGURATION COMMANDS

38 MSTP CONFIGURATION COMMANDS

45 CPOS INTERFACE CONFIGURATION COMMANDS

46 ARP CONFIGURATION COMMANDS

57 DNS CONFIGURATION COMMANDS

58 IP ACCOUNTING CONFIGURATION COMMANDS

59 IP ADDRESSING CONFIGURATION COMMANDS

60 IP PERFORMANCE CONFIGURATION COMMANDS

66 NAT-PT CONFIGURATION COMMANDS

70 TERMINAL ACCESS CONFIGURATION COMMANDS

71 IP ROUTING TABLE COMMANDS

72 BGP CONFIGURATION COMMANDS

73 BGP DEBUGGING COMMANDS

74 IS-IS CONFIGURATION COMMANDS

77 RIP CONFIGURATION COMMANDS

78 ROUTING POLICY COMMON CONFIGURATION COMMANDS

83 IPv6 IS-IS Configuration Commands

84 IPv6 OSPFv3 Configuration Commands

85 IPv6 RIPng Configuration Commands

86 IPv6 Static Routing Configuration Commands

87 Multicast Routing and Forwarding Configuration Commands

88 IGMP CONFIGURATION COMMANDS

89 MSDP CONFIGURATION COMMANDS

90 PIM CONFIGURATION COMMANDS

91 IPv6 MULTICAST ROUTING AND FORWARDING CONFIGURATION COMMANDS

92 MLD CONFIGURATION COMMANDS

93 IPV6 PIM CONFIGURATION COMMANDS

94 MULTICAST VPN CONFIGURATION COMMANDS

95 MPLS BASICS CONFIGURATION COMMANDS

96 MPLS TE CONFIGURATION COMMANDS

97 MPLS L2VPN CONFIGURATION COMMANDS

98 MPLS L3VPN CONFIGURATION COMMANDS

99 VAM SERVER CONFIGURATION COMMANDS

100 VAM CLIENT CONFIGURATION COMMANDS

101 IPSEC PROFILE CONFIGURATION COMMANDS

102 DVPN TUNNEL CONFIGURATION COMMANDS

103 GRE CONFIGURATION COMMANDS

104 L2TP CONFIGURATION COMMANDS

111 FIFO QUEUING CONFIGURATION COMMANDS

112 PQ CONFIGURATION COMMANDS

113 CQ CONFIGURATION COMMANDS

114 WFQ CONFIGURATION COMMANDS

115 CBQ CONFIGURATION COMMANDS

116 RTP PRIORITY QUEUE CONFIGURATION COMMANDS

125 FR QoS Configuration Commands

126 802.1x Configuration Commands

127 AAA Configuration Commands

128 RADIUS CONFIGURATION COMMANDS

129 HWTACACS CONFIGURATION COMMANDS

130 PACKET FILTER FIREWALL CONFIGURATION COMMANDS

131 ASPF CONFIGURATION COMMANDS

132 MAC AUTHENTICATION CONFIGURATION COMMANDS

133 NAT CONFIGURATION COMMANDS

134 PKI CONFIGURATION COMMANDS

135 PORTAL CONFIGURATION COMMANDS

136 RSH CONFIGURATION COMMANDS

137 COMMON CONFIGURATION COMMANDS

138 IPV4 ACL CONFIGURATION COMMANDS

139 IPV6 ACL CONFIGURATION COMMANDS

140 IPSEC CONFIGURATION COMMANDS

141 IKE CONFIGURATION COMMANDS

142 SSH2.0 CONFIGURATION COMMANDS

143 SFTP CONFIGURATION COMMANDS

144 SSL CONFIGURATION COMMANDS

145 BACKUP CENTER CONFIGURATION COMMANDS

146 IPV4-BASED VRRP CONFIGURATION COMMANDS

147 VRRP CONFIGURATION COMMANDS FOR IPV6

148 DEVICE MANAGEMENT COMMANDS

149 NQA CLIENT CONFIGURATION COMMANDS

150 NQA SERVER CONFIGURATION COMMANDS

151 NETSTREAM CONFIGURATION COMMANDS

152 NTP CONFIGURATION COMMANDS

153 RMON CONFIGURATION COMMANDS

154 SNMP CONFIGURATION COMMANDS

155 FILE SYSTEM CONFIGURATION COMMANDS

156 CONFIGURATION FILE MANAGEMENT COMMANDS

157 FTP SERVER CONFIGURATION COMMANDS

158 FTP CLIENT CONFIGURATION COMMANDS

159 TFTP CLIENT CONFIGURATION COMMANDS

164 USER INTERFACE CONFIGURATION COMMANDS

165 MAC Address Table Management Configuration Commands

166 PoE Configuration Commands

167 OAP Module Configuration Commands

168 ACFP CONFIGURATION COMMANDS

169 ACSEI SERVER CONFIGURATION COMMANDS

170 ACSEI CLIENT CONFIGURATION COMMANDS

171 TRACK CONFIGURATION COMMANDS

172 IPX CONFIGURATION COMMANDS

173 VoIP Configuration Commands

174 DIAL PLAN CONFIGURATION COMMANDS

175 E1 AND T1 CONFIGURATION COMMANDS

176 FAX OVER IP CONFIGURATION COMMANDS

177 H.323 CONFIGURATION COMMANDS

178 SIP CONFIGURATION COMMANDS

179 VoFR Configuration Commands

180 Voice RADIUS Configuration Commands

About This Guide

This manual covers the command line interface (CLI) of the H3C MSR 20/30/50 Series routers. It provides a detailed description of the operating commands, which are organized by feature. An alphabetical listing of all commands can be found beginning on page 75.

This manual is intended for the following readers:

- Network administrators
- network engineers
- Users who are familiar with the basics of networking

Always download the Release Notes for your product from the 3Com World Wide Web site and check for the latest updates to software and product documentation: ***http://www.3Com.com***

Conventions

Table 1 lists icon conventions that are used throughout this guide.

Table 1 Notice Icons

Icon	Notice Type	Description
	Information note	Information that describes important features or instructions.
	Caution	Information that alerts you to potential loss of data or potential damage to an application, system, or device.
	Warning	Information that alerts you to potential personal injury.

Table 2 lists text conventions that are used throughout this guide.

Table 2 Text Conventions

Convention	Description
`Screen displays`	This typeface represents information as it appears on the screen.
Keyboard key names	If you must press two or more keys simultaneously, the key names are linked with a plus sign (+), for example: Press Ctrl+Alt+Del
The words "enter" and "type"	When you see the word "enter" in this guide, you must type something, and then press Return or Enter. Do not press Return or Enter when an instruction simply says "type."

Table 2 Text Conventions

Convention	Description
Words in *italics*	Italics are used to: Emphasize a point. Denote a new term at the place where it is defined in the text. Identify menu names, menu commands, and software button names. Examples: From the *Help* menu, select *Contents*. Click *OK*.
Words in **`bold`**	Boldface type is used to highlight command names. For example, "Use the **`display user-interface`** command to..."

Related Documentation

The following manuals offer additional information necessary for managing your MSR 20/30/50 Series router:

- *H3C MSR 20/30/50 Series Routers Installation Manuals* — Covers setting up and initializing your router.
- *H3C MSR 20/30/50 Series Routers Configuration Guide* — Describes how to operate the router. It includes sections about getting started, system management, interface, link layer protocol, network protocol, routing protocol, multicast protocol, security, VPN, reliability, QoS, dial-up and VoIP, as well as acronyms used in the manual.
- *H3C MSR 20/30/50 Series Routers Interface Card and Interface Module Manual* — Covers the pinouts, function, interface attributes, panels, and LEDs of all interface cards and modules available with the router.
- *LMR Series Routers Cable Manual* — Describes the pinouts of the cables available for LMR series routers.
- *Release Notes* — Contains the latest information about your product. If information in this guide differs from information in the release notes, use the information in the Release Notes.

These documents are available in Adobe Acrobat Reader Portable Document Format (PDF) on the CD-ROM that accompanies your router or on the 3Com World Wide Web site: http://www.3Com.com

Alphabetical Listing of Commands

1 PUBLIC ATM AND DSL INTERFACE COMMANDS

display interface atm

Syntax **display interface atm** [*interface-number*]

View Any view

Parameter *interface-number:* Interface number. If no interface is specified, the configuration and status information about all ATM/DSL interfaces and channels on them is displayed.

Description Use the **display interface atm** command to display the configuration and status information about an ATM interface or a DSL interface.

If no interface is specified, this command displays the configuration and status information about all ATM interfaces and DSL interfaces.

Example # Display the configuration and state information about interface ATM 2/0.

```
<Sysname> display interface atm 2/0
Atm2/0 current state :DOWN
Line protocol current state :DOWN
Description :  Atm2/0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
AAL enabled: AAL5, Maximum VCs: 128
Current VCs: 0 (0 on main interface)
ATM over E1, Scramble enabled, frame-format crc4-adm
code hdb3, clock slave,Cable-length long, loopback not set
Cable type:  75 ohm non-balanced
Line Alarm: LOS LOF
Line Error: 0 FERR, 0 LCV, 0 CERR, 0 FEBE
 Last 0 seconds input  rate 0.00 bytes/sec, 0.00 packets/sec
 Last 0 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
 Input : 0 packets, 0 bytes, 0 buffers
         0 errors, 0 crcs, 0 lens, 0 giants,
         0 pads, 0 aborts, 0 timeouts
         0 overflows, 0 overruns,0 no buffer
 Output: 0 packets, 0 bytes, 0 buffers
         0 errors, 0 overflows, 0 underruns
```

interface atm

Syntax **interface atm** *interface-number*

View System view

Parameter *interface-number*: ATM or DSL interface number or DSL interface view.

Description Use the **interface atm** command to enter ATM interface view.

Example # Enter ATM 2/0 interface view.

```
<Sysname> system-view
[Sysname] interface atm 2/0
[Sysname-Atm2/0]
```

reset atm interface

Syntax **reset atm interface** [**atm** *interface-number*]

View User view

Parameter **atm** *interface-number*: Specifies an ATM interface.

Description Use the **reset atm interface** command to clear the statistics on the PVCs created on an ATM interface or all the ATM interfaces.

Note that:

- If you execute this command with an ATM interface specified, this command displays the statistics on the PVCs created on the ATM interface.
- If you execute this command with no ATM interface specified, the statistics on the PVCs created on all the ATM interfaces are cleared.

To clear statistics about ATM interfaces, use the **reset counters interface** command, which is described in *Ethernet Interface Commands* in the *Access Volume*.

Example # Clear the statistics on all the PVCs created on ATM 2/0 interface.

```
<Sysname> reset atm interface atm 2/0
```

2 IMA-E1/T1 Interface Configuration Commands

cable

Syntax **cable** { **long** | **short** }

undo cable

View ATM E1/T1 interface view

Parameter **long**: Long haul mode, with a cable length in the range 151 to 500 m (495 to 1640 ft.).

short: Short haul mode, with a cable length in the range 0 to 150 m (0 to 495 ft.).

Description Use the **cable** command to set the cable length of the ATM E1 interface.

Use the **undo cable** command to restore the default.

By default, long haul mode applies, allowing of cable length mode adaptation. In this case, the long haul mode is adopted first. If the cable is of short haul mode, the system switches to the short haul mode automatically.

To have the system use the short haul mode, use the **cable short** command.

Related command: **frame-format**.

Example # Set the cable length of ATM E1 interface 5/0 to long haul.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] cable long
```

clock

Syntax **clock** { **master** | **slave** }

undo clock

View ATM E1/T1 interface view

Parameter **master**: Sets the clock mode as master.

slave: Sets the clock mode as slave.

Description Use the **clock** command to set the clock mode for an ATM E1/T1 interface.

Use the **undo clock** command to restore the default, that is, the slave clock mode.

For ATM E1/T1 interfaces operating as DCEs, set the clock mode to master. For interfaces operating as DTEa, set the clock mode to slave.

When the ATM interfaces on two routers are connected directly through a fiber-optic cable, set the clock mode to master at one end and to slave at the other end.

Example # Set the clock mode of ATM E1/T1 interface 5/0 to master.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] clock master
```

code

Syntax In ATM E1 interface view:

code { **ami** | **hdb3** }

In ATM T1 interface view:

code { **ami | b8zs** }

undo code

View ATM E1/T1 interface view

Parameter **ami**: Sets the ATM E1/T1 line coding format as AMI.

hdb3: Sets the ATM E1/T1 line coding format as HDB3.

b8zs: Sets the ATM E1/T1 line coding format as B8ZS.

Description Use the **code** command to set the line coding format for an ATM E1/T1 interface.

Use the **undo code** command to restore the default line coding format.

By default, the line coding format of an ATM E1 interface is HDB3, and that of an ATM T1 interface is B8ZS.

Use the **code** command to set the line coding format for an ATM E1/T1 interface.

Use the **undo code** command to restore the default line coding format.

By default, the line coding format of an ATM E1 interface is HDB3, and that of an ATM T1 interface is B8ZS.

Example # Set the line coding format to AMI for ATM 5/0 interface.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] code ami
```

differential-delay

Syntax **differential-delay** *milliseconds*

undo differential-delay

View IMA group interface view

Parameter *milliseconds*: Maximum differential delay, in the range 25 to 100 milliseconds.

Description Use the **differential-delay** command to set the maximum differential delay for the member links in the IMA group.

Use the **undo differential-delay** command to restore the default, that is, 25 milliseconds.

Example # Set the maximum differential delay for the member links in IMA group 1 to 25 milliseconds.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] differential-delay 25
```

display interface ima-group

Syntax **display interface ima-group** [*group-interfacenumber*]

View Any view

Parameter *group-interfacenumber*: IMA group interface number.

Description Use the **display interface ima-group** command to display the configuration and status information about an IMA group interface or all the IMA group interfaces.

If you specify the *group-interfacenumber* argument, this command displays the configuration and status information about the IMA group interface identified by the argument. Otherwise, this command displays the configuration and status information about all the IMA group interfaces.

Example # Display the status and configuration information about IMA group interface 3.

```
<Sysname> display interface ima-group 5/3
Ima-group5/3 current state :DOWN
Line protocol current state :DOWN
Description :  Ima-group3 Interface
Total available baudrate is 1544000 bps,the baudrate now is 1544000 bps
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
AAL enabled: AAL5, Maximum VCs: 128
Current VCs: 0 (0 on main interface)
Physical layer is ATM over IMA
IMA-clock: CTC, active-links-minimum: 1
Frame-length: 128, differential-delay-maximum: 25
symmetry: symmetrical configuration and operation

 Ima-group state:
    ImaGroupNeState          START_UP      ImaGroupFeState          START_UP
    ImaGroupNeFailureStatus  START_UP      ImaGroupFeFailureStatus  START_UP
 Ima-Link state:
    IMA Link Number :  1 , First Link: 0
 Test Status: Disabled

 Last 300 seconds input  rate 0.00 bytes/sec, 0.00 packets/sec
 Last 300 seconds output rate 0.00 bytes/sec, 0.00 packets/sec
 Input : 0 packets, 0 bytes, 0 buffers
         0 errors, 0 crcs, 0 lens, 0 giants,
         0 pads, 0 aborts, 0 timeouts
         0 overflows, 0 overruns,0 no buffer
 Output: 0 packets, 0 bytes, 0 buffers
         0 errors, 0 overflows, 0 underruns
```

frame-format

Syntax In ATM E1 interface view:

frame-format { **crc4-adm** | **no-crc4-adm** }

In ATM T1 interface view:

frame-format { **esf-adm** | **sf-adm** }

undo frame-format

View ATM E1/T1 interface view

Parameter **crc4-adm**: Sets the ATM over E1 framing format to 4-bit cyclic redundancy check ATM direct mapping (CRC4 ADM).

no-crc4-adm: Sets the ATM over E1 framing format to no-CRC4 ADM.

esf-adm: Sets the ATM over T1 framing format to extended super frame ADM (ESF ADM).

sf-adm: Sets the ATM over T1 framing format to super frame ADM (SF ADM).

Description Use the **frame-format** command to configure the ATM over E1/T1 framing format.

Use the **undo frame-format** command to restore the default, that is, CRC4 ADM for ATM E1 interfaces and ESF ADM for ATM T1 interfaces.

ATM Direct Mapping (ADM) directly maps ATM cells transmitted over the E1/T1 line into E1/T1 frames. This process is defined by ITU-T G.804 and ATM forum.

Example # Configure no-CRC4 ADM framing on ATM E1 interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] frame-format no-crc4-adm
```

frame-length

Syntax **frame-length** { **32** | **64** | **128** | **256** }

undo frame-length

View IMA group interface view

Parameter **32**, **64**, **128**, **256**: Specifies the number of ATM cells in an IMA frame.

Description Use the **frame-length** command to configure the number of ATM cells in an IMA frame.

Use the **undo frame-length** command to restore the default, that is, 128 ATM cells in an IMA frame.

Example # Set the number of ATM cells in an IMA frame to 64 on IMA group interface 1.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] frame-length 64
```

ima ima-group

Syntax **ima ima-group** *group-number*

undo ima ima-group

View ATM E1/T1 interface view

Parameter *group-number*: IMA group number, in the range 1 to 8.

Description Use the **ima ima-group** command to add an ATM E1/T1 interface to an IMA group. If the specified IMA group does not exist, it is created first.

Use the **undo ima ima-group** command to remove an interface from an IMA group.

By default, no IMA group is created.

Before adding an ATM E1/T1 interface to an IMA group, you need to remove the network layer service-related configurations of the interface. for example, the IP address assigned to the interface by using the **undo ip address** command.

The first link in the IMA group is the primary link. You can remove it only when you remove the IMA group.

Example # Add the link of ATM E1 interface 5/0 to IMA group 1.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
```

ima-clock

Syntax **ima-clock** { **ctc** [**link-number** *number*] | **itc** }

undo ima-clock

View IMA group interface view

Parameter **ctc**: Common transmit clock configuration. In this mode, all links in the IMA group share the same clock source, which can be an external clock or the one extracted from a member link.

link-number *number*: Number of the E1/T1 link that provides the clock source. It ranges from 0 to 7.

itc: Independent transmit clock configuration. In this mode, the links in the IMA group use at least two clock sources.

Description Use the **ima-clock** command to configure the clock mode of the IMA group.

Use the **undo ima-clock** command to restore the default, that is, CTC.

When the IMA group adopts ITC mode, you must set the clock mode of each member ATM E1/T1 link to slave with the **clock slave** command.

When the IMA group adopts CTC mode, you must set the clock mode of each member ATM E1/T1 link to master with the **clock master** command.

Example # Set the clock mode to ITC on IMA group 1.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] ima-clock itc
```

ima-standard

Syntax **ima-standard { alternate-v10 | normal | standard-v10 | standard-v11 }**

undo ima-standard

View IMA group interface view

Parameter **alternate-v10**: Uses V1.0 (other implementation) standard.

normal: Uses V1.1 standard. An IMA group interface adopting this standard changes to adopt V1.0 (standard implementation) standard if its peer interface adopts V1.0 (standard implementation).

standard-v10: Uses V1.0 (standard implementation) standard.

standard-v11: Uses V1.1 standard.

Description Use the **ima-standard** command to set the standard to be adopted by an IMA group interface.

Use the **undo ima-standard** command to restore the default.

By default, V1.1 standard is adopted.

Example # Configure to adopt V1.1 standard.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] ima-standard standard-v11
```

ima-test

Syntax **ima-test** [**link-number** *number*] [**pattern-id** *id*]

undo ima-test

View IMA group interface view

Parameter **link-number** *number*: Specifies the number of the E1/T1 link to be tested.

pattern-id *id*: Specifies the test mode, a hexadecimal number in the range 0x00 to 0xFE.

Description Use the **ima-test** command to specify the E1/T1 link to be tested and the test mode for IMA group interface test.

Use the **undo ima-test** command to cancel the test.

By default, IMA group interface test is disabled.

Note that:

- If you do not specify the *number* argument, the **ima-test** command specifies to test the link that is the first to be added to the IMA group interface.
- If you do not specify the *id* argument when executing the **ima-test** command, the default test mode (that is, 0xAA) is adopted.
- You can use this command to test the connectivity of a link to the rest of the IMA group by sending a test pattern over the link. This test mode is looped over all the active links at the far end and back to the transmitter. To display the connectivity test result, perform the **display interface ima-group** command.

E1/T1 links are bidirectional. This command tests only the connectivity of a link in its transmit direction to the other links in the IMA group in their receive direction.

Example # Send test mode 0xAB over link 0 in IMA group interface 1.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] ima-test link-number 0 pattern-id ab
```

interface ima-group

Syntax **interface ima-group** *group-interfacenumber*

View System view

Parameter *group-interfacenumber*: IMA group interface number.

Description Use the **interface ima-group** command to enter IMA group interface view.

Example # Enter IMA group interface 1 view.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] quit
[Sysname] interface ima-group 5/1
[Sysname-Ima-group5/1]
```

loopback

Syntax **loopback** { **cell** | **local** | **payload** | **remote** }

undo loopback

View ATM E1/T1 interface view

Parameter **cell**: Internal cell loopback for checking that the local physical chip is operating.

local: Internal loopback for checking that the local service chip is operating.

payload: External payload loopback for checking that payload framing is normal.

remote: External loopback for checking that the remote end is normal.

Description Use the **loopback** command to configure the loopback mode on the ATM E1/T1 interface.

Use the **undo loopback** command to disable loopback.

By default, loopback is disabled.

Example # Enable external payload loopback on ATM E1/T1 interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] loopback payload
```

min-active-links

Syntax **min-active-links** *number*

undo min-active-links

View IMA group interface view

Parameter *number*: Number of links, in the range 1 to 8.

Description Use the **min-active-links** command to configure the minimum number of links required for the IMA group to work.

Use the **undo min-active-links** command to restore the default, that is, 1.

Example # Set the minimum number of links required for IMA group 1 to operate to 2.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] ima ima-group 1
[Sysname-Atm5/0] interface ima-group 5/1
[Sysname-Ima-group5/1] min-active-links 2
```

scramble

Syntax **scramble**

undo scramble

View ATM E1/T1 interface view

Parameter None

Description Use the **scramble** command to enable payload scrambling on the ATM E1/T1 interface. This, however, does not affect cell headers.

Use the **undo scramble** command to disable payload scrambling.

By default, payload scrambling is enabled on an ATM E1/T1 interface.

Example # Enable payload scrambling on ATM interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] scramble
```

3 ATM E3/T3 Interface Configuration Commands

cable

Syntax **cable** { **long** | **short** }

undo cable

View ATM T3 interface view

Parameter **long**: Long haul mode, with a cable length in the range 151 to 500 m (495 to 1640 ft.).

short: Short haul mode, with a cable length in the range 0 to 150 m (0 to 495 ft.).

Description Use the **cable** command to configure the cable length of the ATM T3 interface.

Use the **undo cable** command to restore the default.

By default, short haul mode applies.

Example # Set the cable length of ATM T3 interface 5/0 to long haul.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] cable long
```

clock

Syntax **clock** { **master** | **slave** }

undo clock

View ATM E3/T3 interface view.

Parameter **master**: Sets the clock mode as master.

slave: Sets the clock mode as slave.

Description Use the **clock** command to set the clock mode of the ATM E3/T3 interface.

Use the **undo clock** command to restore the default, that is, the slave clock mode.

Example # Set the clock mode of ATM E3/T3 interface 5/0 to master.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] clock master
```

frame-format

Syntax In ATM E3 interface view:

frame-format { **g751-adm** | **g751-plcp** | **g832-adm** }

In ATM T3 interface view:

frame-format { **cbit-adm** | **cbit-plcp** | **m23-adm** | **m23-plcp** }

undo frame-format

View ATM E3/T3 interface view

Parameter **g751-adm**: Sets the framing format of ATM E3 to G.751 ATM direct mapping (G.751 ADM).

g751-plcp: Sets the framing format of ATM E3 to G.751 physical layer convergence protocol (G.751 PLCP).

g832-adm: Sets the framing format of ATM E3 to G.832 ADM.

cbit-adm: Sets the framing format of ATM T3 to C-bit ADM.

cbit-plcp: Sets the framing format of ATM T3 to C-bit PLCP.

m23-adm: Sets the framing format of ATM T3 to M23 ADM.

m23-plcp: Sets the framing format of ATM T3 to M23 PLCP.

Description Use the **frame-format** command to configure the framing format of the ATM E3/T3 interface.

Use the **undo frame-format** command to restore the default, that is, G.751 PLCP for ATM E3 interfaces and C-bit PLCP for ATM T3 interfaces.

Example # Set the framing format of ATM E3 interface 5/0 to G.832 ADM.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] frame-format g832-adm
```

loopback

Syntax **loopback { cell | local | payload | remote }**

undo loopback

View ATM E3/T3 interface view

Parameter **cell:** Internal cell loopback, used to check whether the local end physical chipset is working properly

local: Internal loopback, used to check whether the local service chip is working properly.

payload: External payload loopback, used to check whether payload framing is normal.

remote: External line loopback, used to check whether the remote end is working properly.

Description Use the **loopback** command to configure the loopback mode on the ATM E3/T3 interface.

Use the **undo loopback** command to disable loopback.

By default, loopback is disabled.

Example # Enable external payload loopback on ATM E3/T3 interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] loopback payload
```

scramble

Syntax **scramble**

undo scramble

View ATM E3/T3 interface view

Parameter None

Description Use the **scramble** command to enable payload scrambling on the ATM E3/T3 interface. This, however, does not affect cell headers.

Use the **undo scramble** command to disable payload scrambling.

By default, payload scrambling is enabled on an ATM E3/T3 interface.

Example # Disable payload scrambling on ATM E3/T3 interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] undo scramble
```

4 ATM OC-3c/STM-1 Interface Configuration Commands

clock

Syntax **clock** { **master** | **slave** }

undo clock

View ATM OC-3c interface view, STM-1 interface view

Parameter **master**: Sets the clock mode as master.

slave: Sets the clock mode as slave.

Description Use the **clock** command to set the clock mode for an ATM OC-3c/STM-1 interface.

Use the **undo clock** command to restore the default, that is, the slave clock mode.

When the ATM interface is operating as DCE, set its clock mode to master. When the interface is operating as DTE, set its clock mode to slave.

When the ATM interfaces on two routers are connected directly through a fiber-optic cable, set the clock mode to master at one end and to slave at the other end.

Example # Set the clock mode of ATM interface 5/0 to master.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] clock master
```

frame-format

Syntax **frame-format** { **sdh** | **sonet** }

undo frame-format

View ATM OC-3c interface view, STM-1 interface view

Parameter **sdh**: Sets the framing format to SDH STM-1, the synchronous transport module-level 1 (STM-1) of synchronous digital hierarchy (SDH).

sonet: Sets the framing format to SONET OC-3, the optical carrier level three (OC-3 of synchronous optical network (SONET).

Description Use the **frame-format** command to set the framing format for an ATM OC-3c/STM-1 interface.

Use the **undo frame-format** command to restore the default, that is, SDH STM-1.

Example # Set the framing format to SDH STM-1 on an ATM OC-3c/STM-1 interface.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] frame-format sdh
```

loopback

Syntax **loopback** { **cell** | **local** | **remote** }

undo loopback

View ATM OC-3c interface view, STM-1 interface view

Parameter **cell**: Enables internal cell loopback.

local: Enables internal loopback.

remote: Enables external loopback.

Description Use the **loopback** command to configure the loopback mode on the ATM OC-3c/STM-1 interface.

Use the **undo loopback** command to disable loopback.

By default, loopback is disabled.

Loopback is intended for test use. Disable it otherwise.

Example # Enable internal loopback on ATM interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] loopback local
```

scramble

Syntax **scramble**

undo scramble

View ATM OC-3c interface view, STM-1 interface view

Parameter None

Description Use the **scramble** command to enable payload scrambling on the ATM OC-3c/STM-1 interface. This, however, does not affect cell headers.

Use the **undo scramble** command to disable payload scrambling.

By default, payload scrambling is enabled on the ATM OC-3c/STM-1 interface.

Example # Enable payload scrambling on ATM interface 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] scramble
```

5 G.SHDSL Interface Configuration Commands

activate

Syntax **activate**

undo activate

View ATM (G.SHDSL) interface view

Parameter None

Description Use the **activate** command to activate the G.SHDSL interface.

Use the **undo activate** command to deactivate the G.SHDSL interface.

By default, a G.SHDSL interface is active.

A G.SHDSL interface must be activated before it can transmit services. Activation refers to training between the G.SHDSL office end and the STU-C end. During this process, the two parties examine line distance and conditions against the line configuration template (which defines the ADSL criteria, channel mode, uplink and downlink speeds, and noise tolerance) and attempt to reach an agreement. If the training succeeds, a communication connection is set up between the two parties.

Contrary to activation, deactivation tears down the communication connection between the two parties. To transmit services, you need to re-activate the interface.

The commands here are intended for test and diagnosis purposes. Unlike the **shutdown** and **undo shutdown** commands, the commands here only affect a G.SHDSL line.

Since a G.SHDSL interface is always on, it transits to the active state automatically at boot and remains in this state as long as the link is in good condition. The router tests the performance of the line regularly. Once it finds that the line performance is deteriorating, it automatically deactivates, retrains, and then reactivates the line.

Example # Activate Atm 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] activate
```

display dsl configuration

Syntax **display dsl configuration interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a iG.SHDSL interface to view the configuration information about.

Description Use the **display dsl configuration** command to display actual GSHDSL configurations.

Example # Display the actual configurations of G.SHDSL interface ATM 3/0.

```
<Sysname> display dsl configuration interface atm 3/0
 GSHDSL line parameter and mode Configuration
 Mode:           CPE
 Standard:       G.991.2
 Annex:          B
 Wire Type:      2
 Framing:        3
 Line Rate:      Auto Adaptive
Current Margin: 2
 SNEXT margin:   0
 Psd Mode:       Sym PSD
 LinkCheck:      Disable

  --Actual Handshake Status --
 00: 0002 0000 0000 0000 0000 0000 0000 0000 0000 0000
 10: 0000 0008 0000 0000 0000 0000 0000 0000 0008 0000
 20: 0000 0000 0002 0002 0004 0010
  --Local Handshake Status --
 00: 0002 0001 0000 0000 0000 0000 0034 003f 003f 003f
 10: 003f 003f 0003 0034 003f 003f 003f 003f 003f 0003
 20: 0000 0000 0003 0003 000f 0010
  --Remote Handshake Status --
 00: 0002 0000 0000 0000 0000 0000 0030 003f 003f 003f
 10: 003f 000f 0000 0030 003f 003f 003f 003f 000f 0000
 20: 0000 0000 0003 0003 0004 0010
```

Table 1 Description on the fields of the display dsl configuration command

Field	Description
Mode	Operating mode, customer premises equipment (CPE) or central office (CO)
Standard	The supported standard
Annex	Available options are **a** and **b**.
Wire Type	Two-wire system or four-wire system.
Framing	Framing format
SNR Threshold	Signal to noise ratio threshold
Current Margin	Current margin
SNEXT margin	Worst-case margin

Table 1 Description on the fields of the display dsl configuration command

Field	Description
Target Margin	Target margin
Line Rate	Line rate
PSD Mode	Power spectral density mode: symmetric or asymmetric
Power-Backoff	Power compensation
LinkCheck	State of link check: enable or disable
Actual Handshake Status	--
Local Handshake Status	--
Remote Handshake Status	--

display dsl status

Syntax **display dsl status interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a G.SHDSL interface to view the status information about.

Description Use the **display dsl status** command to display status information about the specified G.SHDSL interface.

Example # Display status information about ATM 5/0, which is a two-wire G.SHDSL interface that is up.

```
<Sysname> display dsl status interface atm 5/0
 Operating Mode: CPE
DSL Mode:  SHDSL Annex B
Configured Wire Type:   2
Line A Statistics since last activation:
 CRC:            0
 LOSW Defect:    0
 ES:             0
 SES:            0
 UAS:            0
 TX EOC:         0
 RX EOC:         0

 Line A status:
 Xcvr Op State:  Data Mode
 Last Fail Op State:     0x00
 Frame Sync:             in sync
 Line Rate(Kbps):        2312
 Wire Type:              2
 SNR Margin(dB): 16.30
 Loop Attenuation(dB):   0.00
 RecvGain(dB):           6.07
 TxPower(dBm):           9.50
 Power Backoff:  enable
 Power Backoff Level:    5
 Tip/Ring Reversal:      Reversed
 FrmOH Stat:             0x00
 Rmt Encoder A : 0x0000016e
```

```
 Rmt Encoder B : 0x00000331
 Rmt NSF Cusdata :       0x0000
 Rmt NSF CusID : 0x0000
 Rmt Country Code :      0x00b5
 Rmt Provider Code:      GSPN
 Rmt Vendor Data:        0x12 0x34 0x56 0x78
                         0x12 0x34 0x56 0x78
```

Display status information about ATM 5/0, which is a four-wire G.SHDSL interface that is up.

```
<Sysname> display dsl status interface atm 5/0
 Operating Mode:         CPE
 DSL Mode:               SHDSL Annex B
 Configured Wire Type:   4

 Line A Statistics since last activation:
 CRC:            0
 LOSW Defect:    0
 ES:             0
 SES:            0
 UAS:            0
 TX EOC:         0
 RX EOC:         0

 Line A status:
 Xcvr Op State:  Data Mode
 Last Fail Op State:     0x00
 Frame Sync:             in sync
 Line Rate(Kbps):        2312
 Wire Type:              4
 SNR Margin(dB): 13.30
 Loop Attenuation(dB):   0.00
 RecvGain(dB):           5.86
 TxPower(dBm):           9.50
 Power Backoff:  enable
 Power Backoff Level:    5
 Tip/Ring Reversal:      Reversed
 FrmOH Stat:             0x00
 Rmt Encoder A : 0x0000016e
 Rmt Encoder B : 0x00000331
 Rmt NSF Cusdata :       0x0000
 Rmt NSF CusID : 0x0000
 Rmt Country Code :      0x00b5
 Rmt Provider Code:      GSPN
 Rmt Vendor Data:        0x12 0x34 0x56 0x78
                         0x12 0x34 0x56 0x78
Line B Statistics since last activation:
 CRC:            1
 LOSW Defect:    1
 ES:             1
 SES:            1
 UAS:            0
 TX EOC:         0
 RX EOC:         0

 Line B status:
 Xcvr Op State:  Data Mode
 Last Fail Op State:     0x00
 Frame Sync:             in sync
 Line Rate(Kbps):        2312
 Wire Type:              4
 SNR Margin(dB): 12.30
 Loop Attenuation(dB):   0.00
 RecvGain(dB):           5.28
```

```
TxPower(dBm):           9.50
Power Backoff:  enable
Power Backoff Level:    5
Tip/Ring Reversal:      Reversed
FrmOH Stat:             0x00
Rmt Encoder A : 0x0000016e
Rmt Encoder B : 0x00000331
Rmt NSF Cusdata :       0x0000
Rmt NSF CusID : 0x0000
Rmt Country Code :      0x00b5
Rmt Provider Code:      GSPN
Rmt Vendor Data:        0x12 0x34 0x56 0x78
                        0x12 0x34 0x56 0x78
```

Table 2 Description on the fields of the display dsl status command

Field	Description
Operating Mode	CPE or CO
DSL Mode	Annex standard used on the interface: Annex A or Annex B
Configured Wire Type	Configured wire mode of the interface: two-wire or four-wire
Line A Statistics since last activation	Statistics about wire-pair A from the time of initiating to present
CRC	Count of CRC errors
LOSW Defect	Count of loss of synchronization word defects
ES	Error second, count of errors per second
SES	Severely error second, count of severe errors per second
UAS	Unavailable second, count of one-second intervals for which the G.SHDSL line is unavailable
TX EOC	Count of transmitted EOC cells
RX EOC	Count of received EOC cells
Line A status	State of wire-pair A
Xcvr Op State: Data Mode	Operating state of the receiver
Last Fail Op State	Operating state of the receiver when the last negotiation failed
Frame Sync	State of frame synchronization
Line Rate(Kbps)	Negotiated wire-pair speed
Wire Type	Wire type: four-wire, or two-wire
SNR Margin(dB)	Margin to SNR
Loop Attenuation(dB)	Loop attenuation
RecvGain(dB)	Receive gain
TxPower(dBm)	Transmit power
Power Backoff	State of power compensation
Power Backoff Level	Level of power compensation
Tip/Ring Reversal	State of Tip/Ring reverse
FrmOH Stat	Frame outflow state
Rmt Encoder A	Encoding coefficient A
Rmt Encoder B	Encoding coefficient B
Rmt NSF Cusdata	Remote NSF user data
Rmt NSF CusID	Remote NSF user ID
Rmt Country Code	Remote country code

Table 2 Description on the fields of the display dsl status command

Field	Description
Rmt Provider Code	Remote code of the chip provider
Rmt Vendor Data	Remote code of the chip vendor

display dsl version

Syntax **display dsl version interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a G.SHDSL interface to view the version and support capability information about it.

Description Use the **display dsl version** command to display the version and support capability information about the specified G.SHDSL interface.

Example # Display the G.SHDSL version of G.SHDSL interface ATM 5/0.

```
<Sysname> display dsl version interface atm 5/0
 Dsl Line Type:          G.SHDSL
 ATM SAR Device:         0x823614f1
 ATM SAR Revision:       0x02
 Chipset Vendor:         GSPN
 Firmware Rel-Rev:       R2.3.1-0
 DSP Version:            1
 PCB Version:            0.0
 CPLD Version:           0.0
 Driver Version:         2.0
 Hardware Version:       1.0
 ITU G991.2 ANNEX A:     Supported
 ITU G991.2 ANNEX B:     Supported
```

Table 3 Description on the fields of the display dsl version interface atm command

Field	Description
Dsl line Type	Type of the user access line
ATM SAR Device	Identifier of the SAR chip
ATM SAR Revision	Revision identifier of the SAR chip
Chipset Vendor	Identifier of the DSL chipset vendor
Firmware Rel-Rev	Identifier and version of the firmware
DSP Version	--
PCB Version	--
CPLD Version	Logic version
Driver Version	Driver software version
Hardware Version	--
ITU G991.2 ANNEX A, ITU G991.2 ANNEX B	Standards and the annexes supported by the interface

shdsl annex

Syntax **shdsl annex** { **a** | **b** }

undo shdsl annex

View ATM (G.SHDSL) interface view

Parameter **a**: Annex A.

b: Annex B.

Description Use the **shdsl annex** command to configure the annex standard supported on the G.SHDSL interface. You cannot activate a link with different standard types at its two ends.

Use the **undo shdsl annex** command to restore the default, that is, Annex B.

Annex A is dominant in North America while Annex B is dominant in Europe. When setting annex standard, you must consider the standard adopted in the region where your network is located. When ATU-C and ATU-R use different standards, G.SHDSL cannot set up connection.

Example # Configure G.SHDSL interface ATM 5/0 to support annex A.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl annex a
```

shdsl mode

Syntax **shdsl mode** { **co** | **cpe** }

undo shdsl mode

View ATM (G.SHDSL) interface view

Parameter **co**: Specifies the central office (CO) mode.

cpe: Specifies the customer premises equipment (CPE) mode.

Description Use the **shdsl mode** command to set the operating mode for a G.SHDSL interface.

Use the **undo shdsl mode** command to restore the default.

By default, a G.SHDSL interface operates in CPE mode.

For a back-to-back connection, you need to configure one end to CO mode and the other end to CPE mode.

Example # Set the operating mode of interface ATM 5/0 to CO.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl mode co
```

shdsl psd

Syntax **shdsl psd** { **asymmetry** | **symmetry** }

undo shdsl psd

View ATM (G.SHDSL) interface view

Parameter **asymmetry**: Specifies the asymmetric mode, where different power spectral densities (PSD) are set for the central office (CO) and the customer premises equipment (CPE).

symmetry: Specifies the symmetric mode, where the same PSD is set for the CO and CPE.

Power spectral density (PSD) is the amount of power per unit (density) of frequency (spectral) as a function of the frequency. PSD describes how the power of a time series is distributed with frequency.

Description Use the **shdsl psd** command to set PSD of the G.SHDSL interface working as CPE. It is not necessarily the same as the one set at CO.

Use the **undo shdsl psd** command to restore the default.

By default, the PSD of the G.SHDSL interface is in symmetric mode.

Example # Set the PSD of G.SHDSL interface ATM 5/0 to asymmetric mode.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl psd asymmetry
```

shdsl rate

Syntax **shdsl rate** { **auto** | *rate* }

undo shdsl rate

View ATM (G.SHDSL) interface view

Parameter **auto**: Auto-negotiation mode

rate: Maximum single-pair rate of the G.SHDSL interface, in the range of 64 to 2,312, in units of kbps.

- *For four-wire (dual-pair) G.SHDSL, the interface rate is two times single-pair rate. For example, if you set single-pair rate to 2,312 kbps, four-wire interface rate is 4,624 kbps.*
- *Because four-wire G.SHDSL interfaces cannot negotiate rate, do not set their single-pair interface rate to **auto** mode.*

Description Use the **shdsl rate** command to set the single-pair interface rate of the SHDSL interface.

Use the **undo shdsl rate** command to restore the default, that is, **auto**.

In actual applications, likelihood exists that the maximum downlink rate could not reach the specified rate as restricted by ATU-C and line conditions. If you select the **auto** mode, CPE and CO can negotiate a rate commensurate with the current line condition during the activating process. If fixed rates are set at the two ends, the two parties negotiate a rate. In case the lower rate between them cannot be provided, the line could not be activated.

By default, the rate of two-wire G.SHDSL interface is set to auto-negotiation mode; the single-pair interface rate of four-wire G.SHDSL interface is set to 2,312 kbps (four-wire G.SHDSL interface rate is 4,624 kbps).

Example # Configure ATM 5/0 to operate in the auto-negotiation mode.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl rate auto
```

shdsl snr-margin

Syntax **shdsl snr-margin** [**current** *current-margin-value*] [**snext** *snext-margin-value*]

undo shdsl snr-margin

View ATM (G.SHDSL) interface view

Parameter *current-margin-value*: Sets a target margin, in the range 0 to 10. During SHDSL line training, this target margin is considered in addition to the signal-to-noise ratio (SNR) threshold. A larger margin value means increased link stability and noise suppression ability.

snext-margin-value: Sets a target margin, in the range 0 to 10. During SHDSL line training, this target margin is considered in addition to the SNEXT threshold. A larger margin value means increased link stability and noise suppression ability.

Description Use the **shdsl snr-margin** command to set a target margin to signal-to-noise ratio (SNR).

Use the **undo shdsl snr-margin** command to restore the default.

Setting margin can affect maximum rate of the line. When line condition is good, you can set a small margin to obtain higher rate. When much noise is around the line, this may cause disconnection however.

By default, *current-margin-value* is set to 2 and *snext-margin-value* is set to 0.

Example # Set the SNR target margin to 5 on interface ATM 5/0.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl snr-margin current 5
```

shdsl wire

Syntax **shdsl wire** { **2** | **4-auto-enhanced** | **4-enhanced** | **4-standard** }

undo shdsl wire

View ATM (G. SHDSL) interface view

Parameter **2**: Two-wire mode.

4-auto-enhanced: Four-wire auto-switch mode. When this mode is enabled, the four-wire enhanced mode is used first when the local end negotiates with the remote end. If the remote end is not operating in four-wire enhanced mode, the local end uses the four-wire standard mode for negotiation. When four-wire auto-switch mode is adopted, the remote end can be set to operate in four-wire enhanced mode or four-wire standard mode.

4-enhanced: Four-wire enhanced mode. In this mode, the two pairs of the four wires can start negotiation separately; in addition, the remote end must be set to operate in four-wire enhanced mode as well.

4-standard: Four-wire standard mode. In this mode, the two pairs of these four wires must start negotiation at the same time; in addition, the remote end must be set to operate in four-wire standard mode as well.

Description Use the **shdsl wire** command to set the operating mode of the current G.SHDSL interface.

Use the **undo shdsl wire** command to restore the default.

By default, the four-wire G.SHDSL interface operates in four-wire enhanced mode.

*The **shdsl wire** command is available for four-wire G.SHDSL devices only.*

Example # Set four-wire G.SHDSL interface ATM 5/0 to operate in four-wire auto-switch mode.

```
<Sysname> system-view
[Sysname] interface atm 5/0
[Sysname-Atm5/0] shdsl wire 4-auto-enhanced
```

6 ADSL Interface Configuration Commands

activate

Syntax **activate**

undo activate

View ATM (ADSL) interface view

Parameter None

Description Use the **activate** command to activate an ADSL interface.

Use the **undo activate** command to deactivate an ADSL interface.

By default, an ADSL interface is active.

An ADSL interface must be activated before it can transmit services. Activation refers to training between ADSL office end and ATU-R end. During this process, the two parties examine line distance and conditions against the line configuration template (which defines the ADSL criteria, channel mode, uplink and downlink speeds, and noise tolerance) and attempt to reach an agreement. If the training succeeds, a communication connection is set up between the two parties for service transmission.

Contrary to activation, deactivation tears down the communication connection between the two parties. To transmit services, you need to re-activate the interface.

The commands here are intended for test and diagnosis purposes. Unlike the **shutdown** and **undo shutdown** commands, the commands here only affects a G.SHDSL line.

Since an ADSL interface is always on, it transits to the active state automatically at boot and remains in this state as long as the link is in good condition. The router tests the performance of the line regularly. Once it finds that the line performance is deteriorating, it automatically deactivates, retrains, and then reactivates the line.

Example # Activate ADSL interface 2/0.

```
<Sysname> system-view
[Sysname] interface atm 2/0
[Sysname-Atm2/0] activate
```

adsl standard

Syntax **adsl standard** { **auto** | **g9923** | **g9925** | **gdmt** | **glite** | **t1413** }

undo adsl standard

View ATM (ADSL) interface view

Parameter **auto**: Auto-negotiation mode.

g9923: ADSL2 (G992.3) standard.

g9925: ADSL2+ (G992.5) standard.

gdmt: G.DMT (G992.1) standard.

glite: G.Lite (G992.2) standard.

t1413: T1.413 standard.

Description Use the **adsl standard** command to set the standard applied to an ADSL interface.

Use the **undo adsl standard** command to restore the default, that is, auto-negotiation.

Note that:

- ADSL-I module does not support G.Lite (G992.2) standard and T1.413 standard.
- To bring the standard configured by the **adsl standard** command into effect immediately, you need to re-activate the interface by either the **shutdown** and **undo shutdown** commands or the **activate** and **undo activate** commands.

Example # Apply the standard T1.413 to ATM interface 2/0.

```
<Sysname> system-view
[Sysname] interface atm 2/0
[Sysname-Atm2/0]adsl standard t1413
[Sysname -Atm2/0] shutdown
[Sysname -Atm2/0]undo shutdown
```

adsl tx-attenuation

Syntax **adsl tx-attenuation** *attenuation*

undo adsl tx-attenuation

View ATM (ADSL) interface view

Parameter *attenuation*: Transmit power attenuation, in the range 0 to 12.

Description Use the **adsl tx-attenuation** command to set a transmit power attenuation for the ADSL interface.

Use the **undo adsl tx-attenuation** command to restore the default, that is, 0.

Example # Set the transmit power attenuation to 10 for ATM ADSL interface 2/0.

```
<Sysname> system-view
[Sysname] interface atm 2/0
[Sysname-Atm2/0] adsl tx-attenuation 10
```

bootrom update file

Syntax **bootrom update file** *file-url* **slot** *slot-no-list* [**subslot** *subslot-no-list*] [**all** | **part**]

View User view

Parameter *file-url*: File name (including the path) of the software to be upgraded, a string of 1 to 135 characters.

slot *slot-no-list*: List of slot numbers, representing multiple cards. The argument *slot-no-list* appears in the form of { *slot-no* [to *slot-no*] }&<1-7>, where *slot-no* is the slot number of a card, in the range of 1 to the maximum slot number, and &<1-7> means that you can specify up to 7 slot numbers or slot number ranges for this argument. The maximum slot number differs with device models.

subslot *subslot-no-list*: List of sub-slot numbers, representing multiple sub-cards. The argument *subslot-no-list* appears in the form of { *subslot-no* [to *subslot-no*] }&<1-7>, where *subslot-no* is the sub-slot number of a sub-card, in the range of 1 to the maximum sub-slot number, and &<1-7> means that you can specify up to 7 slot numbers or slot number ranges for this argument. The maximum sub-slot number differs with device models.

part: Upgrades only the extension part of the Boot ROM.

all: Upgrades the entire Boot ROM.

Description Use the **bootrom update file** command to upgrade software on an ADSL2+ card.

By default, the entire BootROM is upgraded.

This feature is only valid for ADSL2+ cards with CPUs.

The upgradeable software includes Boot ROM and ADSL2+ card software. Before you do that, you first need to FTP or load the new software file by other means to the Flash or CF card on your device and save it. Before performing an upgrade, you need to shut down the interface with the **shutdown** command if the interface is up. After completing the upgrade, you need to bring the interface up with the **undo shutdown** command.

Use the **all** keyword with caution. In case failure occurs, recovery is difficult and troublesome.

Note that:

- Only distributed devices support the slot slot-no-list option.
- The **subslot** *subslot-no-list* option is not available if the device does not support the sub-card-level maintenance.

Example # Upgrade software for an ADSL2+ card.

```
<Sysname> system-view
[Sysname]interface atm 2/0
[Sysname-Atm2/0]shutdown
[Sysname-Atm2/0] quit
[Sysname] quit
<Sysname> bootrom update file flash:/bcm6348.bin slot 1 part
This command will update BootRom file on board 2, Continue? [Y/N]y
 Board 2 upgrading BOOTROM, please wait...
<Sysname> system-view
[Sysname]interface atm 2/0
[Sysname-Atm2/0]undo shutdown
```

display dsl configuration

Syntax **display dsl configuration interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a DSL interface to view the configuration information about.

Description Use the **display dsl configuration** command to display the configuration of a DSL interface.

Example # Display the actual configurations of ADSL interface ATM 2/0.

```
<Sysname> display dsl configuration interface atm 2/0

 Line Params Set by User
 Standard:               T1.413
 Annex:                  A
 Framing:                3
 Coding Gain(dB):        Auto
 Tx Pow Attn(dB):        0
 Bit-Swap:               disable
 LinkCheck:              Enable

 Actual Config           Near End        Far End
 Standard:               T1.413          T1.413
 Trellis Coding:         Enable          Enable
 Framing:                3               3
 Vendor ID:              0x0039          0x0004
```

```
                          AS0 (DS)        LS0(US)
 Rate(Bytes):             238             26
 Rate(kbps):              7616            832
 Latency:                 Intlv           Intlv
 FEC(fast):               0               0
 S/D/R(Inlv):             1/64/16         8/8/16

 DMT Bits Allocation Per Bin (Up/Down Bits:249/2148)
 00: 0 0 0 0 0 0 7 8 a a a a 8 a b c c c b b b b b b 9 9 a a 9 8 8 0
 20: 0 0 0 0 2 2 2 3 4 4 5 6 6 7 7 8 8 8 8 8 9 9 a a a a a a a 8 9 a
 40: 0 a a a a b b b b b a b b b b b b b b b b b b b b b b b b b b b
 60: b b b b b b b b b b b b b b b b b b b a 9 4 a b b b b b b b b b
 80: b b b b b b b b b b b b b b b b b b b b b b b b b b b b b b b b
 a0: b b b a b a b a b b a b b b b b a a b a a b b a a a a a a a a a
 c0: a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a a
 e0: a 9 9 a 9 9 9 9 9 9 8 9 9 9 9 9 9 9 9 8 8 8 8 8 7 7 7 7 6 6 6
```

Table 4 Description on the fields of the display dsl configuration command

Field	Description
Line Params Set by User	Line parameters at ATU-R end, such as Standard, DMT Mode, Framing, and Trellis Coding. Among these parameters, you can only modify Standard for test or diagnosis, but not the others.
The following information appears after the line is activated.	
Actual Config	Real operating parameters after the line is activated
Rate(kbps)	Negotiation rate in kbps, with AS0 (DS) for the downlink and LS0 (US) for the uplink
Latency	Latency mode: Fast or Interleave
DMT Bits Allocation Per Bin	Bits allocated to and carried by each bin.

display dsl status

Syntax **display dsl status interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a DSL interface to view the status information about.

Description Use the **display dsl status** command to display the status information of a specified DSL interface.

Example # Display the status information of the ADSL interface ATM 2/0.

```
<Sysname> display dsl status interface atm 2/0
Line Status:            Loss Of Signal
 Training Status:        Idle

 Active Params           Near End        Far End
 Standard:               G.dmt           G.dmt
 SNR (dB):               0.0             0.0
 Attn(dB):               0.0             0.0
 Pwr(dBm):               0.0             0.0
```

```
 Current Rate(kbps):      0                0
Latency:                 Intl             Intl
```

Table 5 Description on the fields of the display dsl status command

Field	Description
Line Status	Line status of the ADSL interface, which can be: ■ No Defect, indicating the normal state ■ Loss Of Frame, indicating an error concerning frame ■ Loss Of Signal, indicating an error concerning signal ■ Loss Of Power, indicating an error concerning power supply ■ Loss Of Signal Quality, indicating an error concerning signal quality ■ Unknown, indicating an unknown error
Training Status	Training status of the ADSL interface, which can be: ■ Idle, indicating the interface is idle ■ G.994 Training, indicating a G.994 training ■ G.992 Started, indicating a G.992 training is launched ■ G.922 Channel Analysis, indicating G.922 channel analysis is going on ■ G.992 Message Exchange, indicating G.992 message exchange is going on ■ Showtime, indicating normal data exchange ■ Unknown
The following information appears after the line is activated.	
Active Params	■ Standard, connection standard adopted by the interface and the DSLAM ■ SNR, signal-to-noise ration of the ADSL link ■ Attr, attenuation of the ADSL link ■ Pwr, transmit power of the ADSL module, in dbm ■ Current Rate, uplink/downlink rate between the ADSL interface and the DSLAM, in kbps ■ Latency, Way in which the interface and the DSLAM are connected, which can be “Intl” (cross-over) and “Fast”

display dsl version

Syntax **display dsl version interface atm** *interface-number*

View Any view

Parameter *interface-number*: Specifies a DSL interface to view the version and support capability information on it.

Description Use the **display dsl version** command to display the DSL version and support capabilities of an interface.

Example # Display the ADSL version information of interface ATM 2/0.

```
<Sysname> display dsl version interface atm 2/0
Adsl board chipset and version info:
```

```
 Dsl Line Type:          Adsl Over Pots
 Chipset Vendor:         BDCM
 FW Release:             A2pB017l.d15h
 DSP Version:            17.1200
AFE Version:            1.0
 Bootrom Version:        1.1
 Hardware Version:       4.0
 Driver Version:         1.3
 CPLD Version:           1.0

 Adsl Capability
 ANNEX Supported :
  ANNEX A
 Standard Supported :
  ANSI T1.413 Issue 2
  ITU G992.1(G.dmt)
  ITU G992.2(G.lite)
  ITU G992.3(Adsl2)
  ITU G992.3(ReAdsl2)
  ITU G992.5(Adsl2p)
```

Table 6 Description on the fields of the display adsl version command

Field	Description
Adsl board chipset and version info	The components of the interface board and the version
DSL line Type	Type of the user access line
Chipset Vendor	Identifier of the ADSL chipset vendor
FW Release	Identifier and version of the firmware
DSP Version	--
AFE Version	--
PCB Version	--
Driver Version	Version of the driver software
CPLD Version	Version of the logic
Adsl Capability	The standard and annex supported by the interface.

7 POS INTERFACE CONFIGURATION COMMANDS

clock

Syntax **clock { master | slave }**

undo clock

View POS interface view

Parameter **master**: Sets the clock mode of the POS interface to master.

slave: Sets the clock mode of the POS interface to slave.

Description Use the **clock** command to set the clock mode of the POS interface.

Use the **undo clock** command to restore the default, that is, slave.

POS interfaces support two clock modes:

- Master, which uses internal clock signal.
- Slave, which uses line clock signal.

Similar to the DTE/DCE model of synchronous serial interfaces, POS interfaces need to choose a clock mode. When a POS interface on the router is directly connected to another router, the only requirement is that the two sides use different clock modes. In connection to a switch, however, the switch is DCE and uses internal clock, so the POS interface is DTE and must adopt the slave clock mode.

Example # Set the clock mode of interface POS 1/0 to master.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] clock master
```

crc

Syntax **crc { 16 | 32 }**

undo crc

View POS interface view

Parameter **16**: Sets CRC length to 16 bits.

32: Sets CRC length to 32 bits.

Description Use the **crc** command to set the CRC length on the POS interface.

Use the **undo crc** command to restore the default, that is, 32 bits.

Example # Set the CRC length on interface POS 1/0 to 16 bits.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] crc 16
```

display interface pos

Syntax **display interface pos** [*interface-number*]

View Any view

Parameter *interface-number*: Interface number.

Description Use the **display interface pos** command to display the status and configuration information of the specified or all POS interfaces.

Example # Display the status and configuration information of the interface POS 1/0.

```
<Sysname> display interface pos 1/0
Pos1/0 current state: UP
Line protocol current state: UP
Description: Pos0/0/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 13.13.13.14/8 Primary
Link layer protocol is PPP
LCP opened, IPCP opened, IP6CP opened
Physical is Pos1/0, baudrate: 155520000
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Length)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 5 seconds input:  0 bytes/sec 0 packets/sec
    Last 5 seconds output:  0 bytes/sec 0 packets/sec
    1133 packets input, 14004 bytes, 0 drops
    1133 packets output, 14008 bytes, 0 drops
```

Table 7 Description on the fields of the display interface pos command

Field	Description
Pos1/0 current state	Current state of the POS interface
Line protocol current state	Link layer state of the POS interface
Description	Description on the POS interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)	MTU of the POS interface and the interval at which the link layer protocol sends keepalives

Table 7 Description on the fields of the display interface pos command

Field	Description
Internet protocol processing	IP protocol processing capability, enabled or disabled
Link layer protocol is PPP	Link layer protocol of the POS interface and loopback detection state
LCP opened, IPCP opened, IP6CP opened	LCP state, IPCP state, and IPv6CP state
Physical layer is Pos1/0, Baudrate is 155520000 bps	Physical interface and baudrate
Scramble enabled, crc 32, clock slave, loopback not set	Payload scrambling state, CRC count, clock mode, and loopback state on the interface
Output queue : (Urgent queue : Size/Length/Discards)	Output queues: ■ Urgent queue in size/length/discards ■ Protocol queue in size/length/discards ■ FIFO queue in size/length/discards
Output queue : (Protocol queue : Size/Length/Discards)	
Output queue : (FIFO queuing : Size/Length/Discards)	
SDH alarm section layer line layer path layer C2(Rx), C2(Tx) Rx: J0 Tx: J0 Rx: J1 Tx: J1	SDH alarm counters (or SONET alarm counters depending on framing format) for: ■ Section layer alarms, which could be OOF, LOF, and LOS ■ Line layer alarms, which could be AIS and RDI ■ Path layer alarms, which could be LOP, AIS, and RDI ■ Received and transmitted C2 bytes (C2 is the signal flag byte) ■ Received and transmitted J0 overhead bytes (J0 is the section layer trace byte) Received and transmitted J1 overhead bytes (J1 is the path layer trace byte)
SDH error section layer line layer path layer	SDH error counters (or SONET error counters depending on framing format). They are: B1 for section layer errors B2 for line layer errors and M1 for remote line layer errors B3 for path layer errors and G1 for remote path layer errors
Last 5 seconds input rate 0 bytes/sec, 0 bits/sec, 0 packets/sec	Input rate in Bps, bps, and pps in the last five seconds
Last 5 seconds output rate 0 bytes/sec, 0 bits/sec, 0 packets/sec	Output rate in Bps, bps, and pps in the last five seconds
1133 packets input, 14004 bytes, 0 drops	Count of input and discarded traffic in both packets and bytes
1133 packets output, 14008 bytes, 0 drops	Count of output and discarded traffic in both packets and bytes

display ip interface pos

Syntax **display ip interface pos** *interface-number*

View Any view

Parameter *interface-number:* Interface number.

Description Use the **display ip interface pos** command to view the IP-related configuration and status information of the specified POS interface.

Example # Display IP-related status and configuration information about the interface POS 1/0.

```
<Sysname> display ip interface pos 1/0
Pos1/0 current state :UP
Line protocol current state :UP
Internet Address is 13.13.13.13/8 Primary
Broadcast address : 13.255.255.255
The Maximum Transmit Unit : 1500 bytes
ip fast-forwarding incoming packets state is Enabled
ip fast-forwarding outgoing packets state is Enabled
input packets : 5, bytes : 420, multicasts : 0
output packets : 5, bytes : 420, multicasts : 0
TTL invalid packet number:         0
ICMP packet input number:          5
  Echo reply:                      5
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
  Unknown type:                    0
```

display ipv6 interface pos

Syntax **display ipv6 interface pos** *interface-number*

View Any view

Parameter *interface-number:* Interface number.

Description Use the **display ipv6 interface pos** command to view the IPv6-related configuration and status information of the specified POS interface.

Example # Display IPv6-related status and configuration information about the interface POS1/0.

```
<Sysname> display ipv6 interface pos 1/0
Pos1/0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::813D:0:C252:1
  Global unicast address(es):
    22:22::22:22, subnet is 22::/22 [TENTATIVE]
  Joined group address(es):
    FF02::1:FF22:22
    FF02::1:FF52:1
    FF02::2
    FF02::1
  MTU is 4478 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

flag

Syntax **flag** { **c2** | { **j0** | **j1** } { **sdh** | **sonet** } } *flag-value*

undo flag { **c2** | { **j0** | **j1** } { **sdh** | **sonet** } }

View POS interface view

Parameter **c2** *flag-value*: Path signal flag byte, a higher-order path overhead byte used to indicate the multiplex structure of virtual container (VC) frames and property of payload. It is a hexadecimal number in the range 0 to FF.

j0 *flag-value*: Regeneration section trace message, a section overhead byte used to test continuity of the connection between two interfaces at the section level. If the **sdh** keyword is configured, the *flag-value* argument is a string of 1 to 15 hexadecimal digits. If the **sonet** keyword is configured, the argument is a hexadecimal number in the range 0 to FF.

j1 *flag-value*: Path trace message, a higher-order path overhead byte used to test continuity of the connection between two interfaces at the path level. If the **sdh** keyword is configured, the *flag-value* argument is a string of 1 to 15 hexadecimal digits. If the **sonet** keyword is configured, the argument is a string of 1 to 62 characters.

sdh: Sets framing format to SDH.

sonet: Sets framing format to SONET.

CAUTION: *When the length of the string configured for J0 or J1 is less than 15 or 62 characters, the system automatically pad it with hexadecimal 0x0.*

Description Use the **flag** command to set the SONET/SDH overhead bytes.

Use the **undo flag** { **j0** | **j1** } **sdh** command to restore the default SONET/SDH overhead bytes.

By default, the default SDH overhead bytes are used.

The default overhead bytes are as1 follows.

- **c2**: 0x16
- **j0** (SDH): 15 hexadecimal numbers, each of which has the value of 0x0
- **j1** (SDH): 15 hexadecimal numbers, each of which has the value of 0x0
- **j0** (SONET): 0x01
- **j1** (SONET): 62 hexadecimal numbers, each of which has the value of 0x0

Inconsistency between the c2 and j0 settings of a sending POS interface and the receiving POS interface causes alarms.

Related command: **display interface pos**.

Example # Set the SDH overhead byte J0 of POS1/0 interface.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] flag j0 sdh ff
```

frame-format

Syntax **frame-format** { **sdh** | **sonet** }

undo frame-format

View POS interface view

Parameter **sdh**: Sets framing format to synchronous digital hierarchy (SDH).

sonet: Sets framing format to synchronous optical network (SONET).

Description Use the **frame-format** command to configure framing on the POS interface.

Use the **undo frame-format** command to restore the default, that is, SDH.

Example # Set the framing format on interface POS 1/0 to SDH.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] frame-format sdh
```

link-protocol

Syntax **link-protocol** { **fr** [**nonstandard** | **ietf** | **mfr** *interface-number* | **nonstandard**] | **hdlc** | **ppp** }

View POS interface view

Parameter **fr**: Specifies Frame Relay as the link layer protocol of the interface.

ietf: Adopts the IETF encapsulation format. This is the default.

mfr *interface-number*: MFR interface or subinterface number. The specified interface must be one that already exists.

nonstandard: Adopts non-standard compatible encapsulation format.

hdlc: Specifies HDLC as the link layer protocol of the interface.

ppp: Specifies PPP as the link layer protocol of the interface.

Description Use the **link-protocol** command to set the link layer protocol of the interface.

By default, PPP is used.

Example # Specify HDLC as the link protocol of interface POS 1/0.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] link-protocol hdlc
```

loopback

Syntax **loopback** { **local** | **remote** }

undo loopback

View POS interface view

Parameter **local**: Internal loopback.

remote: External loopback.

Description Use the **loopback** command to enable loopback for a POS interface.

Use the **undo loopback** command to disable loopback.

By default, loopback is disabled.

Loopback is intended for test use. Disable it otherwise.

- *If you enable loopback on a POS interface encapsulated with PPP, it is normal that the state of the link layer protocol is reported up.*
- *Loopback and **clock slave** cannot be set at the same time; otherwise, POS interfaces cannot be connected successfully.*

Example # Enable internal loopback on interface POS 1/0.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] loopback local
```

mtu

Syntax **mtu** *size*

undo mtu

View POS interface view

Parameter *size*: Size (in bytes) of the maximum transmission unit (MTU). MTU range and the default value vary with device.

Description Use the **mtu** command to set the MTU size of the POS interface.

Use the **undo mtu** command to restore the default.

The MTU setting of the POS interface can affect the assembly and fragmentation of IP packets on it.

In QoS, the length of queues is limited. If MTU on the interface is too small, there is likelihood for a large packet to be fragmented into so many fragments that the queue cannot hold them and as such discard them. To avoid this situation, you can extend the queue length by using the **qos fifo queue-length** command in interface view. The default queuing mechanism on the interface is FIFO. For more information on how to configure queuing, refer to "FIFO Queuing Configuration Commands" on page 1809.

Related command: **display interface pos**.

Example # Set MTU of POS interface 0/0/0 to 1492.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] mtu 1492
```

scramble

Syntax **scramble**

undo scramble

View POS interface view

Parameter None

Description Use the **scramble** command to enable payload scrambling on the POS interface.

Use the **undo scramble** command to disable payload scrambling.

By default, payload scrambling is enabled.

You may configure payload scrambling to prevent the presence of excessive consecutive 1s or 0s to facilitate line clock signal extraction at the receiving end.

Only when POS interfaces on both ends are enabled with payload scrambling can they be connected successfully.

Example # Enable payload scrambling on interface POS 1/0.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0]scramble
```

threshold

Syntax **threshold** { **sd** | **sf** } *value*

undo threshold { **sd** | **sf** }

View POS interface view

Parameter *value*: Integer in the range 3 to 9.

Description Use the **threshold** command to set the SD (signal degrade) threshold or SF (signal fail) threshold for a POS interface.

Use the **undo threshold** command to restore the default.

If you execute the **threshold** command with the *value* argument set to **X**, the value of the threshold specified can be obtained using this expression: 10e-**X**.

By default, SD threshold is 10e-6 (that is, **X** is 6), and SF threshold is 10e-3 (that is, **X** is 3).

SD and SF alarms are used to indicate the current line performance. The bit error rate threshold of SF is higher than that of SD, meaning when small amount of errors occurs, SD alarms are generated; while when error rate is increased to a certain degree, SF alarms are generated, indicating the line performance is degrading seriously.

Note that SD threshold should be smaller than SF threshold.

Currently, this command is not supported.

Example # Set the SD threshold to 10e-4 for POS 1/0.

```
<Sysname> system-view
[Sysname] interface pos 1/0
[Sysname-Pos1/0] threshold sd 4
```

8 GENERAL ETHERNET INTERFACE CONFIGURATION COMMANDS

combo enable

Syntax **combo enable** { **copper** | **fiber** }

View Ethernet interface view (the port should be a Combo Port)

Parameter **copper**: Indicates that the electrical port is enabled and uses double-twisted pair cable.

fiber: Indicates that the optical port is enabled and uses optical fiber cable.

Description Use the **combo enable** command to specify the state of a single Combo port. When one port is enabled, the other will be automatically disabled.

By default, the electrical port is enabled.

Related command: **display port** combo and **shutdown**.

Example # Specify to enable the electrical port of Gigabit Ethernet 1/0 and use double-twisted pair cable.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0
[Sysname-GigabitEthernet1/0] combo enable copper
```

Specify to enable the optical port of Gigabit Ethernet 1/0 and use optical fiber cable.

```
<Sysname> system-view
[Sysname] interface gigabitethernet 1/0
[Sysname-GigabitEthernet1/0] combo enable fiber
```

description

Syntax **description** *text*

undo description

View Ethernet interface view

Parameter *text*: The description of an Ethernet interface, a string of 1 to 80 characters.

Description Use the **description** command to configure the description of an Ethernet interface.

Use the **undo description** command to remove the description.

Default to interface name followed by the "interface" string.

Example # Configure the description for interface Ethernet 1/0 to "lan-interface".

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] description lan-interface
```

display brief interface

Syntax **display brief interface** [*interface-type* [*interface-number*]] [| { **begin** | **include** | **exclude** } *text*]

View Any view

Parameter *interface-type*: Type of a specified interface.

interface-number: Number of a specified interface.

|: Uses a regular expression to filter output information.

begin: Displays all the configuration information in the line that contains the specified string and all the lines after this line.

include: Displays information that contains the specified string.

exclude: Displays information that does not contain the specified string.

text: Regular expression, in the range of 1 to 256 characters, excluding spaces.

Table 8 Special characters used in regular expressions

Character	Meaning	Notes on Use
^	Boundary matcher for the beginning of a line. This character specifies a string with which a line begins.	The regular expression "^user" matches lines that begin with the string "user". Lines that don t begin with the string "user", for example, "Auser", are not matched.
$	Boundary matcher for the end of a line. This character specifies a string with which a line ends.	The regular expression "user$" matches lines that end with the string "user". Lines that do not end with the string, for example, "userA", are not matched.
.	Full stop, used as the wildcard character, which matches any single character, including space.	None

Table 8 Special characters used in regular expressions

Character	Meaning	Notes on Use
*	Star, which matches the occurrences of the character to the left for zero or multiple times	zo* matches z and zoo.
+	Plus, which matches one or multiple occurrences of the character to the left	zo+ matches zo and zoo, but not z.
-	Hyphen, which is used to connect two numbers or characters. Note that the number to the left of this character need to be larger than the one to the right. When used in a "[" and "]" pair, it represents a range.	1-9" represent a range from 1 to 9 ("1" and "9" included), and a-h represent a range from "a" to "h" ("a" and "h" included).
[ ]	Specifies a range.	[1-36A] matches a character, which can be a number in the range 1 to 36 or character A.
( )	Specifies a group of characters. Usually used with "+" and "*".	(123A) specifies the string "123A". 408(12)+ matchers "40812" or "408121212" (but not "408"). That is, "12" can appear for multiple times.

Description Use the **display brief interface** command to display brief interface information, including simple interface name, link state, protocol link state, protocol type, and main IP address.

- If neither interface type nor interface number is specified, all interface information will be displayed;
- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related command: **interface**.

Example # Display brief information of interface(s).

```
<Sysname> display brief interface
The brief information of interface(s) under route mode:
Interface          Link      Protocol-link  Protocol type    Main IP
Eth1/0             UP        DOWN           ETHERNET         --
Eth1/1             UP        DOWN           ETHERNET         --
NULL0              UP        UP(spoofing)   NULL             --
S2/0               DOWN      DOWN           PPP              --
S2/1               DOWN      DOWN           PPP              --

The brief information of interface(s) under bridge mode:
Interface          Link      Speed     Duplex   Link-type  PVID
Eth4/0             DOWN      auto      auto     access     1
Eth4/1             DOWN      auto      auto     access     1
Eth4/2             DOWN      auto      auto     access     1
Eth4/3             DOWN      auto      auto     access     1
Eth4/4             DOWN      auto      auto     access     1
Eth4/5             DOWN      auto      auto     access     1
```

```
Eth4/6              DOWN      auto      auto     access     1
Eth4/7              DOWN      auto      auto     access     1
```

Display brief interface information that contains the string "UP".

```
<Sysname> display brief interface | include UP
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
Eth0/1             UP        DOWN           ETHERNET         --
Eth0/1             UP        DOWN           ETHERNET         --
NULL0                UP        UP(spoofing)   NULL             --
```

Table 9 Description on the fields of the display brief interface command.

Field	Description
The brief information of interface(s) under route mode:	Brief information of interface(s) in route mode
Interface	Interface name
Link	Interface physical link state, which can be up or down
Protocol-link	Interface protocol link state, which can be up or down
Protocol type	Interface protocol type
Main IP	Main IP
The brief information of interface(s) under bridge mode:	Brief information of interface(s) in bridge mode
Speed	Interface rate, in bps
Duplex	Duplex mode, which can be half (half duplex), full (full duplex), or auto (auto-negotiation).
PVID	Default VLAN ID

Table 10 Acronyms for different types of Interface

Interface name	Acronyms
Ethernet	Eth
GigabitEthernet	GE

display interface

Syntax **display interface** [*interface-type* [*interface-number*]]

View Any view

Parameter *interface-type*: Type of a specified interface.

interface-number: Number of a specified interface.

Description Use the **display interface** command to display the current state of a specified interface and related information.

- If neither interface type nor interface number is specified, all interface information will be displayed;

- If only interface type is specified, then only information of this particular type of interface will be displayed.
- If both interface type and interface number are specified, then only information of the specified interface will be displayed.

Related command: **interface**.

Example # Display the current state of Layer 3 interface Ethernet 1/0 and related information.

```
<Sysname> display interface ethernet 1/0
Ethernet 1/0 current state: DOWN
Line protocol current state: DOWN
Description: Ethernet 1/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e223-82f5
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e223-82f5
Media type is optical fiber, loopback not set, promiscuous mode not set
Speed Negotiation, Duplex Negotiation, link type is autonegotiation
Output flow-control is disabled, input flow-control is disabled
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last clearing of counters: 17:14:08  Tue 05/09/2006
    Last 300 seconds input rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Last 300 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Input: 0 packets, 0 bytes, 0 buffers
           0 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 runts, 0 giants
           0 crc, 0 align errors, 0 overruns
           0 dribbles, 0 drops, 0 no buffers
    Output:0 packets, 0 bytes, 0 buffers
           0 broadcasts, 0 multicasts, 0 pauses
           0 errors, 0 underruns, 0 collisions
           0 deferred, 0 lost carriers
```

Table 11 Description on the fields of the display interface (in route mode) command.

Field	Description
Ethernet1/0 current state	Interface physical link state
Line protocol current state	Interface protocol link state
Description	The description of an Ethernet interface
The Maximum Transmit Unit	The Maximum Transmit Unit
Hold timer	Hold timer of link state
Internet protocol processing	Internet protocol processing
IP Packet Frame Type, Hardware Address	IP Packet Frame Type, Hardware Address
IPv6 Packet Frame Type, Hardware Address	IPv6 Packet Frame Type, Hardware Address
Output queue (Urgent queue : Size/Length/Discards)	Output queue (current message number in the urgent queue/ maximum number of messages allowed in the urgent queue/number of discarded messages)
Output queue (Protocol queue : Size/Length/Discards)	Output queue (current message number in the protocol queue/ maximum number of messages allowed in the protocol queue/number of discarded messages)

Table 11 Description on the fields of the display interface (in route mode) command.

Field	Description
Output queue (FIFO queuing : Size/Length/Discards)	Output queue (current message number in the FIFO queue/ maximum number of messages allowed in the FIFO queue/number of discarded messages)
Last 300 seconds input rate	Average input rate over the last 300 seconds
Last 300 seconds output rate	Average output rate over the last 300 seconds
Input	Input packets
Output	Output packets

Display the current state of Layer 2 interface Ethernet1/0 and related information.

```
<Sysname> display interface ethernet 1/0
Ethernet1/0 current state: DOWN
 IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: 000f-e200-8048
 Description: Ethernet1/0 Interface
 Loopback is not set
 Media type is twisted pair, port hardware type is 100_BASE_TX
 Unknown-speed mode, unknown-duplex mode
 Link speed type is autonegotiation, link duplex type is autonegotiation
 Flow-control is not enabled
 The Maximum Frame Length is 1536
 Broadcast MAX-ratio: 100%
 Unicast MAX-ratio: 100%
 Multicast MAX-ratio: 100%
 PVID: 100
 Mdi type: auto
 Port link-type: access
  Tagged   VLAN ID : none
  Untagged VLAN ID : 100
 Port priority: 0
 Last 300 seconds input:  6 packets/sec 678 bytes/sec     20%
 Last 300 seconds output:  1 packets/sec 179 bytes/sec     17%
 Input (total):  61745144 packets, 12152212250 bytes
          47519150 broadcasts, 12121681 multicasts
 Input (normal):  61745144 packets, - bytes
          47519150 broadcasts, 12121681 multicasts
 Input:  0 input errors, 0 runts, 0 giants, 0 throttles
          0 CRC, 0 frame, - overruns, 0 aborts
          - ignored, - parity errors
 Output (total): 1395522 packets, 183608303 bytes
          13 broadcasts, 1273860 multicasts, 0 pauses
 Output (normal): 1395522 packets, - bytes
          13 broadcasts, 1273860 multicasts, 0 pauses
 Output: 0 output errors, - underruns, 1 buffer failures
          0 aborts, 0 deferred, 0 collisions, 0 late collisions
          0 lost carrier, - no carrier
```

Table 12 Description on the fields of the display interface command (in bridge mode)

Field	Description
Ethernet1/0 current state	Current physical link state of the Ethernet interface
IP Packet Frame Type	Frame type of the Ethernet interface
Hardware address	Hardware address
Description	Description of the interface
Loopback is not set	Loopback is not configured

Table 12 Description on the fields of the display interface command (in bridge mode)

Field	Description
Unknown-speed mode	Unknown-speed mode, in which mode speed is negotiated between the current host and the peer
unknown-duplex mode	unknown-duplex mode, in which mode speed is negotiated between the current host and the peer
Link speed type is autonegotiation	Link speed type is autonegotiation
link duplex type is autonegotiation	Link duplex type is autonegotiation
Flow-control is not enabled	Flow-control is not enabled
The Maximum Frame Length	The maximum frame length allowed on an interface
Broadcast-suppression ratio(%)	Broadcast storm suppression ratio (the maximum ratio of allowed number of broadcast packets to overall traffic through an interface)
Unicast MAX-ratio	Unicast storm suppression ratio (the maximum ratio of allowed number of unknown unicast packets to overall traffic over an interface)
Multicast MAX-ratio	Multicast storm suppression ratio (the maximum ratio of allowed number of multicast packets to overall traffic through an interface)
PVID	Default VLAN ID
Mdi type	Cable type
Port link-type	Interface link type, which could be access, trunk, and hybrid.
Tagged VLAN ID	Identify the VLANs that need Tag markers
Untagged VLAN ID	Identify the VLANs that do not need Tag markers
Last 300 seconds input:	Average input rate over the last 300 seconds, among which: ■ **packets/sec** indicates the average input rate in terms of the average number of the packets received per second. ■ **bytes/sec** indicates the average input rate in terms of the average number of bytes received per second. ■ **x%** indicates the percentage of the average input rate to the total bandwidth, where **-** indicates that the rate is greater than the maximum value that can be displayed.
Last 300 seconds output	Average output rate over the last 300 seconds, among which: ■ **packets/sec** indicates the average output rate in terms of the average number of the packets output per second. ■ **bytes/sec** indicates the average output rate in terms of the average number of bytes output per second. ■ **x%** indicates the percentage of the average output rate to the total bandwidth, where **-** indicates that the rate is greater than the maximum value that can be displayed.

Table 12 Description on the fields of the display interface command (in bridge mode)

Field	Description
Input (total): Input (normal): Input: Output (total): Output (normal): Output:	Error statistics on the interface inbound and outbound packets, underscore indicates that the corresponding entry is invalid

duplex

Syntax **duplex** { **auto** | **full** | **half** }

undo duplex

View Ethernet interface view

Parameter **auto**: Indicates that the interface is in an auto-negotiation state.

full: Indicates that the interface is in a full-duplex state.

half: Indicates that the interface is in a half-duplex state.

Description Use the **duplex** command to configure the duplex mode for an Ethernet interface.

Use the **undo duplex** command to restore the duplex mode for an Ethernet interface to the default.

By default, the duplex mode for an Ethernet interface is auto.

Related command: **speed**.

Example # Configure the interface Ethernet 1/0 to work in full-duplex mode.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] duplex full
```

flow-control

Syntax **flow-control**

undo flow-control

View Ethernet interface view

Parameter None

Description Use the **flow-control** command to turn on flow control on an Ethernet interface.

Use the **undo flow-control** command to turn off flow control on an Ethernet interface.

By default, flow control on an Ethernet interface is turned off.

The flow control can be implemented on the local Ethernet interface only when the flow control function is enabled on both the local and peer devices.

Example # Turn on flow control on interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] flow-control
```

interface

Syntax **interface** *interface-type interface-number*

View System view

Parameter *interface-type interface-number*: Interface type and interface number.

- *Interface is identified by slot number/interface number, for example, Ethernet 1/0 can be represented as 1/0.*
- *For ease of user input, interface type can be abbreviated so long as it does not cause any confusion, for example, interface Ethernet 1/0 can be abbreviated as e1/0.*

Description Use the **interface** command to enter the related interface view.

Example # Enter interface view of the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]
```

loopback

Syntax **loopback** { **external** | **internal** }

undo loopback

View Ethernet interface view

Parameter **external**: Enables external loopback testing on an Ethernet interface. The support for this keyword varies with device models.

internal: Enables internal loopback testing on an Ethernet interface. The support for this keyword varies with device models.

Description Use the **loopback** command to enable Ethernet interface loopback testing.

Use the **undo loopback** command to disable Ethernet interface loopback testing.

By default, Ethernet interface loopback testing is disabled.

- *The support for these two commands varies with device models.*
- *Ethernet interface loopback testing should be enabled while testing certain functionalities, such as during the initial identification of any network failure.*
- *While enabled, Ethernet interface loopback testing will work in a full-duplex mode. The interface will return to its original state upon completion of the loopback testing.*

Example # Configure to enable loopback testing on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] loopback internal
```

port link-mode

Syntax **port link-mode { bridge | route }**

undo port link-mode

View Ethernet interface view

Parameter **bridge**: Works in bridge mode.

route: Works in route mode.

Description Use the **port link-mode** command to change the working mode of the Ethernet interface.

Use the **undo port link-mode** command to restore the original working mode.

According to the layer at which the device processes received data packets, Ethernet interfaces can work in bridge or route mode. For a device, some interfaces can work only in bridge mode, some can work only in route mode, and others can work in bridge mode or route mode. This command is only applicable to Ethernet interfaces whose working mode can be changed.

CAUTION:

- *Only 4SIC-FSW interface cards, 9DSIC-FSW interface cards, and the fixed switching interfaces of 20-21 routers support work mode switching.*
- *On an MSR series router, you can change the working mode to route mode for up to two Ethernet interfaces.*
- *After the working mode is changed, all parameters of the Ethernet interface will be restored to the defaults in the current working mode.*

Example # Configure Ethernet1/0 to work in bridge mode.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] display this
#
interface Ethernet1/0
 port link-mode route
#
return
[Sysname-Ethernet1/0] port link-mode bridge
[Sysname-Ethernet1/0] display this
#
interface Ethernet1/0
 port link-mode bridge
#
return
```

*Use the **display this** command to display the current configurations.*

reset counters interface

Syntax **reset counters interface** [*interface-type* [*interface-number*]]

View User view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **reset counters interface** command to reset statistics for a specified interface.

To sample network traffic within a period of time for an interface, you need to reset the original interface statistics.

- If neither interface type nor interface number is specified, all interface information will be reset;
- If only interface type is specified, then only information of this particular type of interface will be reset.
- If both interface type and interface number are specified, then only information of the specified interface will be reset.

Example # Clear the statistics of Ethernet 1/0.

```
<Sysname> reset counters interface ethernet 1/0
```

shutdown

Syntax **shutdown**

undo shutdown

View Ethernet interface view

Parameter None

Description Use the **shutdown** command to shut down an Ethernet interface.

Use the **undo shutdown** command to turn on Ethernet interface.

In certain circumstances, modification to the interface parameters does not immediately take effect, and therefore, you need to shut down the relative interface to make the modification work.

Example # Shut down the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] shutdown
```

Turn on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo shutdown
```

speed

Syntax **speed** { **10** | **100** | **1000** | **auto** }

undo speed

View Ethernet interface view

Parameter **10**: Indicates that the interface rate is 10 Mbps.

100: Indicates that the interface rate is 100 Mbps.

1000: Indicates that the interface rate is 1000 Mbps.

auto: Indicates that the interface rate is in the auto-negotiation state.

Description Use the **speed** command to configure Ethernet interface data rate.

Use the **undo speed** command to restore Ethernet interface data rate.

By default, Ethernet interface data rate is automatically negotiated between peer Ethernet interfaces.

Note that the following:

- The Combo port does not support the **speed** command.
- The **speed 1000** command is only applicable to Gigabit Ethernet interface.

Related command: **duplex**.

Example # Configure data rate for the interface Ethernet 1/0 to 100 Mbps.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] speed 100
```

9 CONFIGURATION COMMANDS FOR ETHERNET INTERFACES IN BRIDGE MODE

broadcast-suppression

Syntax **broadcast-suppression** { *ratio* | **pps** *max-pps* }

undo broadcast-suppression

View Ethernet interface view, port group view

Parameter *ratio*: Maximal ratio of broadcast traffic to the total transmission capability of an Ethernet interface. Currently, this argument can only be set to 100.

pps *max-pps*: Specifies the maximal broadcast packet number per second for an Ethernet interface, in pps, representing packets per second. Currently, the *max-pps* argument can only be 190, 380, 760, 1488, 2976, 5952, or 11904.

Description Use the **broadcast-suppression** command to configure a broadcast storm suppression ratio.

Use the **undo broadcast-suppression** command to restore the default broadcast storm suppression ratio.

By default, all broadcast traffic is allowed to go through an Ethernet interface, that is, broadcast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configuration takes effect only on the current interface. If you execute this command in port group view, the configuration takes effect on all the ports in the port group.

Note that when broadcast traffic exceeds the maximum value configured, the system will discard the extra packets so that the broadcast traffic ratio falls below the limit to ensure that the network functions properly.

If you set different suppression ratios in Ethernet interface view or port group view repeatedly, the last configuration takes effect.

Example # Set the maximum broadcast traffic allowed on Ethernet1/0 to 5952 pps.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] broadcast-suppression pps 5952
```

display loopback-detection

Syntax **display loopback-detection**

View Any view

Parameter None

Description Use the **display loopback-detection** command to display loopback detection information on a port

If loopback detection is already enabled, this command will also display the detection interval and information on the ports currently detected with a loopback.

Example # Display loopback detection information on a port.

```
<Sysname> display loopback-detection
Loopback-detection is running
Detection interval time is 30 seconds
There is no port existing loopback link
```

Table 13 Description on the fields of the display loopback-detection command.

Field	Description
Loopback-detection is running	Loopback-detection is running
Detection interval time is 30 seconds	Detection interval is 30 seconds
There is no port existing loopback link	No port is currently being detected with a loopback

display port

Syntax **display port** { **hybrid** | **trunk** }

View Any view

Parameter **hybrid**: Displays the current Hybrid port(s).

trunk: Displays the current Trunk port(s).

Description Use the **display port** command to display information on the current ports of a specified type, including port name, default VLAN ID, and the VLAN ID of VLANs that the ports can pass through.

Example # Display the current Hybrid port(s).

```
<Sysname> display port hybrid
Interface            PVID  VLAN passing
Eth1/4             100   Tagged:  1000, 1002, 1500, 1600-1611, 2000,
                                  2555-2558, 3000, 4000
```

```
                                    Untagged:1, 10, 15, 18, 20-30, 44, 55, 67, 100,
                                             150-160, 200, 255, 286, 300-302
```

Display the current Trunk port(s).

```
<Sysname> display port trunk
Interface            PVID  VLAN passing
Eth1/8               2     1-4, 6-100, 145, 177, 189-200, 244, 289, 400,
                           555, 600-611, 1000, 2006-2008
```

Table 14 Description on the fields of the display port command.

Field	Description
Interface	Interface name
PVID	Default VLAN ID of the interface
VLAN passing	VLAN ID of VLANs that the ports can pass through

display port-group manual

Syntax **display port-group manual** [**all** | **name** *port-group-name*]

View Any view

Parameters **all**: Specifies all the manual port groups.

name *port-group-name*: Specifies the name of a manual port group, a string of 1 to 32 characters.

Description Use the **display port-group manual** command to display the information about a manual port group or all the manual port groups.

- If you provide the *port-group-name* argument, this command displays the details of a specified manual port group, including its name and the Ethernet interfaces included.
- If you provide the **all** keyword, this command displays the details of all the manual port groups, including their names and the Ethernet interfaces included.
- If no argument or keyword is specified, this command displays the names of all the existing manual port groups.

Examples # Display the names of all the manual port groups.

```
<Sysname> display port-group manual
The following manual port group exist(s):
group1                                    group2
```

Display the details of all the manual port groups.

```
<Sysname> display port-group manual all
Member of group1:
    Ethernet1/0            Ethernet1/1            Ethernet1/2
    Ethernet1/3            Ethernet1/4            Ethernet1/5
    Ethernet1/6            Ethernet1/7            Ethernet2/0
    Ethernet2/1
```

```
Member of group2:
None
```

Display the details of the manual port group named **group 1**.

```
<Sysname> display port-group manual name group1
Member of group1:
    Ethernet1/0             Ethernet1/1             Ethernet1/2
    Ethernet1/3             Ethernet1/4             Ethernet1/5
    Ethernet1/6             Ethernet1/7             Ethernet2/0
```

Table 15 Description on the fields of the display port-group manual command

Field	Description
Member of group	Member ports of the manual port group

flow-interval

Syntax **flow-interval** *interval*

undo flow-interval

View System view

Parameter *interval*: Time interval at which interface statistics is collected, in the range of 5 to 300 seconds, a multiple of 5. The system default is 300 seconds.

Description Use the **flow-interval** command to configure the time interval for collecting interface statistics.

Use the **undo flow-interval** command to restore the default interval.

Example # Set the time interval for collecting interface statistics to 100 seconds.

```
<Sysname> system-view
[Sysname] flow-interval 100
```

group-member

Syntax **group-member** *interface-list*

undo group-member *interface-list*

View Port group view

Parameters *interface-list*: Ethernet interface list, in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] } &<1-10>, where &<1-10> indicates that you can specify up to 10 interfaces or interface ranges

Description Use the **group-member** command to add specified Ethernet interfaces to a manual port group.

Use the **undo group-member** command to remove specified Ethernet interfaces from a manual port group.

By default, a manual port group contains no Ethernet interface.

Examples # Add interface Ethernet 1/0 to the manual port group named **group 1**.

```
<Sysname> system-view
[Sysname] port-group manual group1
[Sysname-port-group-manual-group1] group-member ethernet 1/0
```

loopback-detection control enable

Syntax **loopback-detection control enable**

undo loopback-detection control enable

View Ethernet interface view

Parameter None

Description Use the **loopback-detection control enable** command to enable loopback detection for a Trunk port or Hybrid port.

Use the **undo loopback-detection control enable** command to restore the default.

By default, loopback detection for a Trunk port or Hybrid port is disabled.

- When the loopback detection is enabled, if a port has been detected with loopback, it will be shutdown. A Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.
- When the loopback detection is disabled, if a port has been detected with loopback, a Trap message will be sent to the terminal. The port is still working properly.

By default, loopback detection for Trunk port and Hybrid port is disabled.

Note that this command is inapplicable to an Access port as its loopback detection is enabled by default.

Example # Enable loopback detection for the Trunk port Ethernet 1/0.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type trunk
[Sysname-Ethernet1/0] loopback-detection enable
[Sysname-Ethernet1/0] loopback-detection control enable
```

loopback-detection enable

Syntax **loopback-detection enable**

undo loopback-detection enable

View System view/Ethernet interface view

Parameter None

Description Use the **loopback-detection enable** command to enable loopback detection globally or on a specified port.

Use the **undo loopback-detection enable** command to disable loopback detection globally or on a specified port.

By default, loopback detection is disabled for an Access, Trunk, or Hybrid port.

- If an Access port has been detected with loopback, it will be shutdown. A Trap message will be sent to the terminal and the corresponding MAC address If a Trunk port or Hybrid port has been detected with loopback, a Trunk message will be sent to the terminal. They will be shutdown if the loopback testing function is enabled on them. In addition, a Trap message will be sent to the terminal and the corresponding MAC address forwarding entries will be deleted.

Related command: **loopback-detection control enable**.

CAUTION:

- *Loopback detection on a given port is enabled only after the **loopback-detection enable** command has been issued in both system view and the **interface** view of the port.*
- *Loopback detection on all ports will be disabled after the issuing of the undo **loopback-detection enable** command under system view.*

Example # Enable loopback detection on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] loopback-detection enable
```

loopback-detection interval-time

Syntax **loopback-detection interval-time** *time*

undo loopback-detection interval-time

View System view

Parameter *time*: Time interval in seconds for port loopback detection, in the range of 5 to 300.

Description Use the **loopback-detection interval-time** command to configure time interval for port loopback detection.

Use the **undo loopback-detection interval-time** command to restore the default time interval for port loopback detection, which is 30 seconds.

Related command: **display loopback-detection**.

Example # Set the time interval for port loopback detection to 10 seconds.

```
<Sysname> system-view
[Sysname] loopback-detection interval-time 10
```

loopback-detection per-vlan enable

Syntax **loopback-detection per-vlan enable**

undo loopback-detection per-vlan enable

View Ethernet interface view

Parameter None

Description Use the **loopback-detection per-vlan enable** command to enable loopback detection in all VLANs with Trunk ports or Hybrid ports.

Use the **undo loopback-detection per-vlan enable** command to enable loopback detection in the default VLAN with Trunk ports or Hybrid ports.

By default, loopback detection is only enabled in the default VLAN(s) with Trunk ports or Hybrid ports.

Note that the **loopback-detection per-vlan enable** command is not applicable to access ports.

Example # Enable loopback detection in all VLANs to which the Hybrid port Ethernet 1/0 belong.

```
<Sysname> system-view
[Sysname] loopback-detection enable
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] loopback-detection enable
[Sysname-Ethernet1/0] port link-type trunk
[Sysname-Ethernet1/0] loopback-detection per-vlan enable

[Sysname-Ethernet1/0] loopback-detection per-vlan enable
```

mdi

Syntax **mdi** { **across** | **auto** | **normal** }

undo mdi

View Ethernet interface view

Parameter **across**: Specifies cross-over cables for the Ethernet interface.

auto: Configures the Ethernet interface to be auto-sensing for the cable type.

normal: Specifies straight-through cables for the Ethernet interface.

Description Use the **mdi** command to configure the cable type that can be sensed by an Ethernet interface.

Use the **undo mdi** command to restore the system default.

By default, an Ethernet interface senses the type of the network cable connected to it automatically.

The optical port of a Combo port does not support this command.

Example # Configure the interface Ethernet 1/0 to use cross over cable.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mdi across
```

multicast-suppression

Syntax **multicast-suppression** { *ratio* | **pps** *max-pps* }

undo multicast-suppression

View Ethernet interface view, port group view

Parameter *ratio*: Maximal ratio of multicast traffic to the total transmission capability of an Ethernet interface, in the range of 1 to 100. Currently, this argument can only be set to 100.

pps *max-pps*: Specifies the maximal number of multicast packets passing an Ethernet interface per second, in pps, representing packets per second. Currently, the *max-pps* argument can only be 190, 380, 760, 1488, 2976, 5952, or 11904.

Description Use the **multicast-suppression** command to configure multicast storm suppression ratio on an interface.

Use the **undo multicast-suppression** command to restore default multicast suppression ratio.

By default, all multicast traffic is allowed to go through an Ethernet interface, that is, multicast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configuration takes effect only on the current interface. If you execute this command in port group view, the configuration takes effect on all ports in the port group.

Note that when multicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the multicast traffic ratio can drop below the limit to ensure that the network functions properly.

If you set different suppression ratios in Ethernet interface view or port group view repeatedly, the last configuration takes effect.

Example # Set the maximum multicast traffic allowed on Ethernet 1/0 to 5952 PPS.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-GigabitEthernet1/0] multicast-suppression pps 5952
```

port-group

Syntax **port-group** { **manual** *port-group-name* | **aggregation** *agg-id* }

undo port-group manual *port-group-name*

View System view

Parameter **manual** *port-group-name*: Specifies the name of a manual port group, a string of 1 to 32 characters.

aggregation *agg-id*: Specifies the ID of an existing port aggregation group. You can use the **display link-aggregation summary** command to display the brief information of all the existing port aggregation groups. The support for this keyword-argument combination varies with device models.

Description Use the **port-group manual** command to create a manual port group and enter manual port group view.

Use the **port-group aggregation** command to enter aggregation group view.

Use the **undo port-group manual** command to remove a manual port group.

By default, no manual port group is created.

Example # Enter manual port group 1 view.

```
<Sysname> system-view
[Sysname] port-group manual group1
```

unicast-suppression

Syntax **unicast-suppression** { *ratio* | **pps** *max-pps* }

undo unicast-suppression

View Ethernet interface view, port group view

Parameter *ratio*: Maximal ratio of unicast traffic to the total transmission capability of an Ethernet interface, in the range of 1 to 100. The smaller the ratio is, the less unicast traffic is allowed through the interface.

pps *max-pps*: Specifies the maximal number of unknown unicast packets passing through an Ethernet interface per second. The *max-pps* argument ranges from 1 to 148,810, in pps, representing packets per second.

Description Use the **unicast-suppression** command to configure a unicast storm suppression ratio.

Use the **undo unicast-suppression** command to restore the default unicast suppression ratio.

By default, all unicast traffic is allowed to go through an Ethernet interface, that is, unicast traffic is not suppressed.

If you execute this command in Ethernet interface view, the configuration takes effect only on the current interface. If you execute this command in port group view, the configuration takes effect on all ports in the port group.

Note that when unicast traffic exceeds the maximum value configured, the system will discard the extra packets so that the unknown unicast traffic ratio can drop below the limit to ensure that the network functions properly.

Currently, these two commands are not supported.

Example # Allow unicast traffic equivalent to 20% of the total transmission capability of the interface to pass through Ethernet 1/0 and suppress the excessive unknown unicast packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] unicast-suppression 20
```

virtual-cable-test

Syntax **virtual-cable-test**

View Ethernet interface view

Parameter None

Description Use the **virtual-cable-test** command to enable the virtual cable test for an Ethernet interface and to display the testing result. The tested items include:

- Cable status: Could be normal, abnormal, abnormal-open, abnormal-short, and failure;
- Cable length;
- Pair Impedance mismatch;
- Pair skew;
- Pair swap;
- Pair polarity;
- Insertion loss;
- Return loss;
- Near-end crosstalk.

By default, virtual cable test is disabled.

Note:

- When the cable is functioning properly, the cable length in the test result represents the total cable length;
- When the cable is not functioning properly, the cable length in the test result represents the length from the current interface to the failed position.

- *The optical interface of a Combo port does not support this command.*
- *A link in the up state goes down and then up automatically if you execute this command on one of the Ethernet interfaces forming the link.*

Example # Enable the virtual cable test for the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] virtual-cable-test
Cable status: abnormal(open), 7 metres
Pair Impedance mismatch: yes
Pair skew: 4294967294 ns
Pair swap: swap
Pair polarity: normal
Insertion loss: 7 db
Return loss: 7 db
Near-end crosstalk: 7 db
```

10 CONFIGURATION COMMANDS FOR ETHERNET INTERFACES IN ROUTE MODE

mtu

Syntax **mtu** *size*

undo mtu

View Ethernet interface view

Parameter *size*: The value of Maximum Transmission Unit (MTU for short), which varies by interface type and defaults to 1,500 bytes.

- Fast Ethernet: (FE for short): in the range of 46 bytes to 1,560 bytes
- GigabitEthernet (GE for short) or 10 GE: in the range of 46 bytes to 16,384 bytes, with a default value of 1,500 bytes.

Description Use the **mtu** command to configure MTU value.

Use the **undo mtu** command to restore MTU value.

Limited to the QoS queue length (for example, the default length of an FIFO queue is 75), too small an MTU will result in too many fragments, which will be discarded from the QoS queue. In this case, you can increase MTU or QoS queue length properly. In Ethernet interface view, you can use ***qos fifo queue-length*** *to change the QoS queue length. For detailed configurations, see "qos fifo queue-length" on page 1809.*

Example # Configure MTU for Ethernet1/0 to be 1,000 bytes.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mtu 1000
```

timer hold

Syntax **timer hold** *seconds*

undo timer hold

View Ethernet interface view

Parameter *seconds*: Time interval in seconds for link suppression, in the range of 0 to 32,767. A value 0 represents the link test is disabled.

Description Use the **timer hold** command to configure Layer 3 Ethernet interface link-layer-state change suppression time.

Use the **undo timer hold** command to restore the default suppression time.

By default, Layer 3 Ethernet link-layer-state change suppression time is set to 10 seconds. Peer Ethernet interfaces have the same suppression time. If both sides set their suppression time to 0, the link-layer-state change suppression time is disabled.

You can increase the polling interval to reduce negative effect on network traffic due to the network time lag or heavy congestion.

Example # Configure the link state change suppression time for the interface Ethernet 1/0 to 20 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] timer hold 20
```

11 FUNDAMENTAL SERIAL INTERFACE CONFIGURATION COMMANDS

async mode

Syntax **async mode** { **flow** | **protocol** }

undo async mode

View Asynchronous serial interface view, AUX interface view, AM interface view

Parameter **flow**: Flow mode, also known as interactive mode. In this mode, the two ends interact attempting to set up a link after the physical link is set up. During this process, the calling party sends configuration commands to the called party (this is equal to the operation of manually inputting configuration commands at the remote end), sets the link layer protocol operating parameters of the called party, and then sets up the link. This approach normally applies to man-machine interaction.

protocol: Protocol mode. In this mode, the interface uses configured link layer protocol parameters to set up link with the remote end after its physical link is set up.

Description Use the **async mode** command to set the operating mode of the current interface.

Use the **undo async mode** command to restore the default.

By default, an asynchronous serial interface operates in protocol mode and an AUX interface operates in flow mode.

You can configure PPP when the asynchronous serial interface is working in flow mode, but the configuration does not take effect. The PPP configuration takes effect only after you change the operating mode of the interface to protocol.

Example # Set asynchronous serial interface 1/0 to operate in flow mode.

```
<Sysname> system-view
[Sysname] interface async 1/0
[Sysname-async1/0] async mode flow
```

baudrate

Syntax **baudrate** *baudrate*

undo baudrate

View Serial interface view

Parameter *baudrate*: Baud rate (in bps) to be set for a serial interface.

Description Use the **baudrate** command to set the baud rate for a serial interface.

Use the **undo baudrate** command to restore the default.

By default, the baud rate is 64,000 bps on a synchronous serial interface.

The following are the baud rates available with synchronous serial interfaces:

1,200 bps, 2,400 bps, 4,800 bps, 9,600 bps, 19,200 bps, 38,400 bps, 56,000 bps, 57,600 bps, 64,000 bps, 72,000 bps, 115,200 bps, 128,000 bps, 192,000 bps, 256,000 bps, 384,000 bps, 512,000 bps, 1,024,000 bps, 2,048,000 bps, and 4,096,000 bps.

The baud rate range available with synchronous serial interfaces depends on the applied physical electric specifications.

- For V.24 DTE/DCE, the baud rate available ranges from 1,200 bps to 64,000 bps.
- For V.35 DCE/DCE, X.21 DTE/DCE, EIA/TIA-449 DTE/DCE, and EIA-530 DTE/DCE, the baud rate available ranges from 1,200 bps to 4,096,000 bps.

CAUTION:

- *Take the physical electric specifications of the cable into consideration when setting the baud rate for a serial interface.*
- *The baud rate adopted by a DCE-DTE pair is determined by the DCE.*

Example # Set the baud rate of synchronous serial interface 1/0 at DCE side to 115,200 bps.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] baudrate 115200
```

clock (serial interface view)

Syntax **clock** { **dteclk1** | **dteclk2** | **dteclk3** | **dteclk4** | **dteclkauto** }

undo clock

View Serial interface view

Parameter **dteclk1**: Sets the interface clock selection mode to DTE clock option 1.

dteclk2: Sets the interface clock selection mode to DTE clock option 2.

dteclk3: Sets the interface clock selection mode to DTE clock option 3.

dteclk4: Sets the interface clock selection mode to DTE clock option 4.

dteclkauto: Sets the interface clock selection mode to DTE autonegotiation.

Description

Use the **clock** command to set clock selection mode for the synchronous serial interface.

Use the **undo clock** command to restore the default.

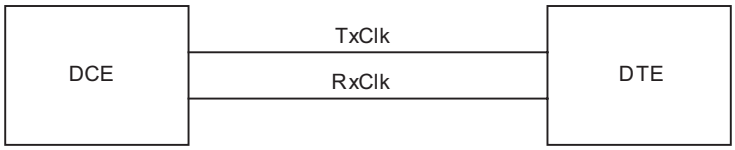
By default, the DTE-side clock on synchronous serial interfaces is DTE clock option 1 (**dteclk1**).

A synchronous serial interface can operate as DCE or DTE.

- As DCE, the interface provides DCEclk clock to the DTE.
- As DTE, the interface accepts the clock provided by the DCE. As transmitting and receiving clocks of synchronization devices are independent, the receiving clock of a DTE device can be either the transmitting or receiving clock of the DCE device, so is the transmitting clock. Therefore, four clock options are available for a DTE device.

See Figure 1:

Figure 1 Select a clock for a synchronous serial interface



In the figure, "TxClk" represents transmitting clock and "RxClk" receiving clock.

The following table gives the four clock selection options.

Table 16 Clock options available for a synchronous serial interface working as DTE

Clock selection option	Description
DTEclk1	TxClk = TxClk, RxClk = RxClk
DTEclk2	TxClk = TxClk, RxClk = TxClk
DTEclk3	TxClk = RxClk, RxClk = TxClk
DTEclk4	TxClk = RxClk, RxClk = RxClk

In the table, the clock ahead of the equal sign (=) is the DTE clock and the one behind is the DCE clock.

Example

Set the synchronous serial interface working as DTE to use the clock selection option **dteclk2**.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] clock dteclk2
```

code nrzi

Syntax **code nrzi**

undo code

View Synchronous serial interface view

Parameter None

Description Use the **code nrzi** command to set the digital signal coding format to none-return-to-zero-inverse (NRZI) on the synchronous serial interface.

Use the **undo code** command to restore the default, that is, NRZ.

Example # Set the digital signal coding format to NRZI on synchronous serial interface 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] code nrzi
```

country-code

Syntax **country-code** *area-name*

undo country-code

View Asynchronous serial interface view, AM interface view

Parameter *area-name*: Area name, which can be australia, austria, belgium, brazil, bulgaria, canada, china, czechoslovakia, denmark, finland, france, germany, greece, hongkong, hungary, india, ireland, israel, italy, japan, korea, luxembourg, malaysia, mexico, netherlands, new-zealand, norway, philippines, poland, portugal, russia, singapore, southafrica, spain, sweden, switzerland, taiwan, united-kingdom, and united-states.

Description Use the **country-code** command to set the coding format of the modem connected to the asynchronous serial or AM interface.

Use the **undo country-code** command to restore the default, that is, united-states.

You may use this command to adapt to the modem coding formats in different countries and areas.

Before you can use this command on an asynchronous serial interface, you must first enable the **modem** command.

Example # Set the country-code to china.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] country-code china
```

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Specifies 16-bit CRC.

32: Specifies 32-bit CRC.

none: Disables CRC.

Description Use the **crc** command to set the CRC mode.

Use the **undo crc** command to restore the default.

By default, 16-bit CRC is adopted.

These two commands are not available to sub-serial interfaces and synchronous/asynchronous serial interfaces operating as asynchronous interfaces.

Example # Configure to adopt 32-bit CRC.

```
<Sysname> system-view
[Sysname] interface serial 0/0/0
[Sysname-Serial0/0/0] crc 32
```

detect

Syntax

1 Asynchronous serial interface

detect dsr-dtr

undo detect dsr-dtr

2 Synchronous serial interface

detect { **dcd** | **dsr-dtr** }

undo detect { **dcd** | **dsr-dtr** }

View Synchronous serial interface view, asynchronous serial interface view

Parameter **dsr-dtr**: Detects DSR (data set ready) and DTR (data terminal ready) signals of DSU/CSU (data service unit/channel service unit).

dcd: Detects the DCD (data carrier detect) signal of the DSU/CSU on the serial interface.

Description Use the **detect** command to enable data carrier detection as well as level detection on the serial interface.

Use the **undo detect** command to disable data carrier detection as well as level detection on the serial interface.

By default, data carrier and level detection is enabled on serial interfaces.

If level detection is disabled on an asynchronous serial interface, the system automatically reports that the state of the serial interface is up with both DTR and DSR being up without detecting whether a cable is connected. If level detection is enabled on the interface, the system detects the DSR signal in addition to the external cable. The interface is regarded up only when the detected DSR signal is valid. Otherwise, it is regarded down.

When determining whether a synchronous serial interface is up or down, the system by default detects the DSR signal, DCD signal, and presence of cable connection. Only when the three signals are all valid will the interface be regarded up. If level detection is disabled, the system considers that the interface is up with both DTR and DSR being up after detecting the cable connection.

*The **modem** command and the **undo detect dsr-dtr** command are mutually exclusive.*

Example # Enable data carrier detection on synchronous serial interface 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] detect dcd
```

eliminate-pulse

Syntax **eliminate-pulse**

undo eliminate-pulse

View Asynchronous serial interface view

Parameter None

Description Use the **eliminate-pulse** command to eliminate the pulses with a width less than 3.472 us, thus increasing signal reliability. This is useful when the line is seriously interfered.

Use the **undo eliminate-pulse** command to restore the default, eliminating the pulses with a width less than 1.472 us.

When the baud rate of the interface is 115,200 bps, you cannot configure this command. After you configure this command, the baud rate of the interface cannot be set to 115,200 bps.

This command is restricted to the 8ASE and 16ASE interface cards and modules.

Example # Eliminate the pulses with a width less than 3.472 us on interface Async 1/0.

```
<Sysname> system-view
[Sysname] interface async 1/0
[Sysname-Async1/0] eliminate-pulse
```

idle-mark

Syntax **idle-mark**

undo idle-mark

View Synchronous serial interface view

Parameter None

Description Use the **idle-mark** command to set the line idle code of the synchronous serial interface to 0xFF.

Use the **undo idle-mark** command to restore the default, that is, 0x7E.

In most cases, a synchronous serial interface uses 0x7E to identify the idle state of the line. You may need to set the line idle code to 0xFF however to interoperate with devices that use 0xFF (high level of all ones) as line idle code.

Example # Set the line idle code of synchronous serial interface 2/0 to 0xFF.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] idle-mark
```

invert receive-clock

Syntax **invert receive-clock**

undo invert receive-clock

View Serial interface view

Parameter None

Description Use the **invert receive-clock** command to invert the receive-clock signal on the DTE-side synchronous serial interface.

Use the **undo invert transmit-clock** command to restore the default.

By default, receive-clock signal inversion is disabled on DTE-side synchronous serial interfaces.

Sometimes, you may need to invert the receive-clock signal on a DTE-side serial interface to eliminate the half clock-period delay on the line. This command is necessary only for some special DCE devices. In common applications, clock must not be inverted.

Related command: **physical-mode**, **invert transmit-clock**, **clock (serial interface view)**.

Example # Invert the receive-clock on DTE-side synchronous serial interface 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] invert receive-clock
```

invert transmit-clock

Syntax **invert transmit-clock**

undo invert transmit-clock

View Serial interface view

Parameter None

Description Use the **invert transmit-clock** command to invert the transmit-clock signal on the DTE-side synchronous serial interface.

Use the **undo invert transmit-clock** command to restore the default.

By default, transmit-clock signal inversion is disabled on DTE-side synchronous serial interfaces.

Sometimes, you may need to invert the receive-clock signal on a DTE-side serial interface to eliminate the half clock-period delay on the line. This command is necessary only for some special DCE devices. In common applications, clock must not be inverted.

Related command: **physical-mode**, **invert receive-clock**, **clock (serial interface view)**.

Example # Invert the transmit-clock on DTE-side synchronous serial interface 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] invert transmit-clock
```

loopback

Syntax **loopback**

undo loopback

View Serial interface view, AUX interface view, AM interface view

Parameter None

Description Use the **loopback** command to enable internal loopback on the serial interface.

Use the **undo loopback** command to restore the default.

By default, loopback is disabled.

Loopback is intended for test use. Disable it otherwise.

Example # Enable internal loopback on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] loopback
```

mtu (on serial interfaces)

Syntax **mtu** *size*

undo mtu

View Serial interface view, AUX interface view, AM interface view, USB interface view

Parameter *size*: Maximum transmission unit (MTU) to be set for a serial interface, in the range 128 to 1,500 (in bytes).

Description Use the **mtu** command to set the MTU for a serial interface.

Use the **undo mtu** command to restore the default.

By default, the MTU of a serial interface is 1,500 bytes.

Due to the length of Qos queue, a packet may be discarded if the MTU is relatively small and the packet is segmented into too many fragments. You can increase the Qos queue length to avoid this situation. To do so, use the **qos fifo queue-length** command in interface view. For details, refer to the "FIFO Queuing Configuration Commands" on page 1809.

The MTU setting can affect IP packets assembly and fragmentation on the interface.

Example # Set the MTU of interface Serial 2/0 to 1,200 bytes.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] mtu 1200
```

physical-mode

Syntax **physical-mode** { **async** | **sync** }

View Serial interface view

Parameter **async**: Sets the synchronous/asynchronous serial interface to operate in asynchronous mode.

sync: Sets the synchronous/asynchronous serial interface to operate in synchronous mode.

Description Use the **physical-mode** command to set the operating mode of the synchronous/asynchronous serial interface.

By default, synchronous/asynchronous serial interfaces are operating in synchronous mode.

Example # Set synchronous/asynchronous serial interface 2/0 to operate in asynchronous mode.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial1/0] physical-mode async
```

phy-mru

Syntax **phy-mru** *size*

undo phy-mru

View Asynchronous serial interface view, AUX interface view

Parameter *size*: Maximum receive unit (MRU) to be set, in the range 4 to 1,700 (in bytes).

Description Use the **phy-mru** command to set the MRU for an asynchronous serial interface operating in flow mode.

Use the **undo phy-mru** command to restore the default.

By default, the MRU of an asynchronous serial interface is 1,700 bytes.

Note that these two commands only apply to interfaces operating in the asynchronous flow mode.

Example # Set the MRU of interface serial 2/0 to 1,500 bytes (assuming that the interface is an asynchronous serial interface and operates in flow mode).

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] physical-mode async
[Sysname-Serial2/0] async mode flow
[Sysname-Serial2/0] phy-mru 1500
```

reverse-rts

Syntax **reverse-rts**

undo reverse-rts

View Synchronous serial interface view

Parameter None

Description Use the **reverse-rts** command to reverse RTS signal for debugging purpose.

Use the **undo reverse-rts** command to restore the default.

By default, RTS signal reverse is disabled.

This command is used in hardware flow control where the remote is not allowed to send data when the local end is doing that.

Example # Reverse RTS signal.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] reverse-rts
```

timer hold

Syntax **timer hold** *seconds*

undo timer hold

View Serial interface view, AUX interface view, AM interface view, USB interface view

Parameter *Seconds*: Link state polling interval (in seconds) to be set, in the range 1 to 32,767.

Description Use the **timer hold** command to set the link state polling interval.

Use the **undo timer hold** command to restore the default.

By default, the link state polling interval is 10 second.

Example # Set the link state polling interval to 20 seconds for interface serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] timer hold 20
```

virtualbaudrate

Syntax **virtualbaudrate** *virtualbaudrate*

undo virtualbaudrate

View Synchronous serial interface view

Parameter *virtualbaudrate*: Baud rate (in bps) to be set, which must be consistent with the one configured at the DCE side. It can be 1,200, 2,400, 4,800, 9,600, 19,200, 38,400, 56,000, 57,600, 64,000, 72,000, 115,200, 128,000, 192,000, 256,000, 384,000, 512,000, 768,000, 2,048,000, or 4,096,000.

Description Use the **virtualbaudrate** command to set a virtual baud rate for the DTE interface.

Use the **undo virtualbaudrate** command to remove the specified virtual baud rate.

When working as DTE, the serial interface determines its baud rate through negotiation with the DCE side. The **virtualbaudrate** command, however, allows you to configure DTE-side baudrate manually, but the configured value must be the same as the one set at the DCE side.

After executing the **virtualbaudrate** command, you need to shut down and then bring up the interface (using the **shutdown** command and the **undo shutdown** command) for the new setting to take effect.

- *Configure the **baudrate** command at DCE side and the **virtualbaudrate** command at DTE side (only when the interface is operating in synchronous mode). Avoid configuring the two commands at the same end of a link.*
- *At DCE side, the **display interface** command displays the baud rate of the interface; whereas at the DTE end, the command displays the virtual baud rate of the interface.*

Related command: **baudrate**.

Example # Set the virtual baudrate of DTE interface Serial 1/0 to 19,200 bps.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] virtualbaudrate 19200
```

12 FUNDAMENTAL CE1/PRI INTERFACE CONFIGURATION COMMANDS

cable

Syntax **cable** { **long** | **short** }

undo cable

View CE1/PRI interface view

Parameter **long**: Indicates that the attenuation of receiver is -43 dB.

short: Indicates that the attenuation of receiver is -10 dB.

Description Use the **cable** command to set the cable type for a CE1/PRI interface.

Use the **undo cable** command to restore the default.

By default, the **long** keyword applies.

Example # Set the cable length matching CE1/PRI interface E1 2/0 to **short**.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] cable short
```

channel-set (CE1/PRI interface view)

Syntax **channel-set** *set-number* **timeslot-list** *list*

undo channel-set [*set-number*]

View CE1/PRI interface view

Parameter *set-number*: The number of the channel set formed by bundling timeslots on the interface, in the range 0 to 30.

timeslot-list *list*: Specifies timeslots to be bundled. The *list* argument is timeslot numbers, in the range of 1 to 31. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*.

Description Use the **channel-set** command to bundle timeslots on the CE1/PRI interface into a channel-set.

Use the **undo channel-set** command to restore the default.

By default, no timeslots are bundled into channel sets.

A CE1/PRI interface in CE1/PRI mode is physically divided into 32 timeslots numbered 0 through 31.

In actual applications, all the timeslots except timeslot 0 can be bundled into multiple channel sets. For each channel set, the system automatically creates a serial interface which is logically equivalent to a synchronous serial interface.

The serial interface is numbered in the form of **serial** *interface-number***:***set-number*, where, *interface-number* is the number of the CE1/PRI interface, and *set-number* is the number of the channel set.

Only one timeslot bundling mode can be supported on a CE1/PRI interface at a time. In other words, this command cannot be used together with the **pri-set** command.

Example # Bundle timeslots 1, 2, 5, 10 through 15, and 18 on CE1/PRI interface E1 2/0 into channel set 0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] channel-set 0 timeslot-list 1,2,5,10-15,18
```

Make the same configuration on the CE1/PRI interface on the remote router.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] channel-set 0 timeslot-list 1,2,5,10-15,18
```

clock (CE1/PRI interface view)

Syntax **clock** { **master** | **slave** }

undo clock

View CE1/PRI interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **clock** command to configure clock source for the CE1/PRI interface.

Use the **undo clock** command to restore the default clock source, that is, line clock.

When the CE1/PRI interface is working as DCE, choose the internal clock (**master**) for it. When it is working as DTE, choose the line clock for it.

Example # Use the internal clock as the clock source on CE1/PRI interface E1 2/0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] clock master
```

code (CEI/PRI interface view)

Syntax **code** { **ami** | **hdb3** }

undo code

View CE1/PRI interface view

Parameter **ami**: Adopts alternate mark inversion (AMI) line code format.

hdb3: Adopts high density bipolar 3 (HDB3) line code format.

Description Use the **code** command to set the line code format for the CE1/PRI interface.

Use the **undo code** command to restore the default, that is, HDB3.

Keep the line code format of the interface in consistency with that used by the remote device.

Example # Set the line code format of interface E1 2/0 to AMI.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] code ami
```

controller e1

Syntax **controller e1** *number*

View System view

Parameter *number*: CE1/PRI interface number.

Description Use the **controller e1** command to enter CE1/PRI interface view.

Example # Enter E1 2/0 interface view.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0]
```

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit cyclic redundancy check (CRC).

32: Adopts 32-bit CRC.

none: Disables CRC.

Description Use the **crc** command to configure CRC mode for a synchronous serial interface formed on a CE1/PRI interface.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

Example # Apply 32-bit CRC to a serial interface formed on interface CE1 interface 2/0 in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] using e1
[Sysname-E1 2/0] quit
[Sysname] interface serial 2/0:0
[Sysname-Serial2/0:0] crc 32
```

detect-ais

Syntax **detect-ais**

undo detect-ais

View CE1 interface view, PRI interface view

Parameter None

Description Use the **detect-ais** command to enable AIS (alarm indication signal) test on an interface.

Use the **undo detect-ais** command to disable AIS test.

By default, AIS test is performed.

Example # Enable AIS test on E1 2/0 interface.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] detect-ais
```

display controller e1

Syntax **display controller e1** [*interface-number*]

View Any view

Parameter *interface-number*: Interface number. In conjunction with the **e1** keyword, it specifies a CE1/PRI interface.

Description Use the **display controller e1** command to display information about one or all the CE1/PRI interfaces.

The displayed information includes:

- Physical state of interface
- Clock mode (source) of interface
- Frame check mode of interface
- Line code format of interface

Example # Display information about interface E1 2/0.

```
<Sysname> display controller e1 2/0
E1 2/0 current state: UP
Description : E1 2/0 Interface
Basic Configuration:
  Work mode is E1 framed, Cable type is 75 Ohm unbalanced.
  Frame-format is no-crc4.
  Line code is hdb3, Source clock is slave.
  Idle code is 7e, Itf type is 7e, Itf number is 4.
  Loop back is not set.
Alarm State:
  Receiver alarm state is None.
Historical Statistics:
Last clearing of counters: Never
    Data in current interval (150 seconds elapsed):
    0 Loss Frame Alignment Secs, 0 Framing Error Secs,
    0 CRC Error Secs, 0 Alarm Indication Secs, 0 Loss-of-signals Secs,
    0 Code Violations Secs, 0 Slip Secs, 0 E-Bit error Secs.
```

Table 17 Description on the fields of the command

Field	Description
E1 2/0 current state: UP	State of the interface
Description : E1 2/0 Interface	Description of the interface
Work mode	Work mode of the interface, which can be E1 or CE1.
Cable type	Cable type of the interface
Frame-format	Frame format of the interface, which can be CRC4 or non-CRC4.
Source Clock	Work mode of the source clock of the interface, which can be master or slave.

Table 17 Description on the fields of the command

Field	Description
Line Code	Line code, which can be AMI or HDB3.
Idle Code	Idle code, which can be 0x7E or 0xFF.
Itf type	Iterframe filling tag, which can be 0x7E or 0xFF.
Itf number	Number of interframe filling tags between two successive frames.
Loopback	Loopback state
Alarm State	Alarm state
Historical Statistics	Statistics on the interface
Last clearing of counters	Indicates whether or not the counters are cleared periodically
Data in current interval (150 seconds elapsed):	Statistics on the errors during the current interval
0 Loss Frame Alignment Secs, 0 Framing Error Secs,	
0 CRC Error Secs, 0 Alarm Indication Secs, 0 Loss-of-signals Secs,	
0 Code Violations Secs, 0 Slip Secs, 0 E-Bit error Secs	

error-diffusion restraint config

Syntax **error-diffusion restraint config** *detect-timer renew-timer threshold*

undo error-diffusion restraint config

View System view

Parameter *detect-timer*: Setting of the error packet detect timer, in the range 30 to 600 (in seconds).

renew-timer: Setting of the renew timer, in the range 120 to 2400 (in seconds).

threshold: Error packet ratio threshold, in the range 5 to 100 (in percentage).

Description Use the **error-diffusion restraint config** command to set the three parameters in error packet diffusion restraint.

Use the **undo error-diffusion restraint enable** command to restore the default settings of the three parameters.

By default, the error packet detect timer is set to 30 seconds, the renew timer is set to 600 seconds, and the error packet ratio threshold is 20.

The setting of renew timer must be at least four times that of the error packet detect timer. If the total number of the packets received during *detect-timer* is less than 100, error packets are not counted.

- *The support for these two commands varies with device models.*
- *These two commands apply to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # Set the error packet detect timer to 100 seconds, the renew timer to 2400 seconds, and the error packet ratio threshold to 15.

```
<Sysname> system-view
[Sysname] error-diffusion restraint config 100 2400 15
```

error-diffusion restraint enable

Syntax **error-diffusion restraint enable**

undo error-diffusion restraint enable

View System view

Parameter None

Description Use the **error-diffusion restraint enable** command to enable error packets diffusion restraint.

Use the **undo error-diffusion restraint enable** command to disable this function.

By default, error packets diffusion restraint is enabled.

- *The support of these two commands varies with device model.*
- *These two commands apply to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # Enable error packets diffusion restraint.

```
<Sysname> system-view
[Sysname] error-diffusion restraint enable
```

error-diffusion restraint restart-channel

Syntax **error-diffusion restraint restart-channel serial** *interface-number*:*set-number*

View System view

Parameter **serial** *interface-number:set-number*: Number of channel formed by bundling CE1/PRI interfaces, where *interface-number* is the number of the CE1/PRI interface, *set-number* is the number of the channel set.

Description Use the **error-diffusion restraint restart-channel** command to restart the channel that has been shut down for the sake of error packets diffusion restraint.

- *The support of this command varies with device model.*
- *This command applies to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # restart channel serial 2/0:0 that has been shut down due to error packets diffusion.

```
<Sysname> system-view
[Sysname] error-diffusion restraint restart-channel serial 2/0:0
```

frame-format (CE1/PRI interface view)

Syntax **frame-format** { **crc4** | **no-crc4** }

undo frame-format

View CE1/PRI interface view

Parameter **crc4**: Sets framing format to CRC4.

no-crc4: Sets framing format to no-CRC4.

Description Use the **frame-format** command to set the framing format on the CE1 interface.

Use the **undo frame-format** command to restore the default, that is, no-CRC4.

A CE1/PRI interface in CE1 mode supports both CRC4 and no-CRC4 framing formats, where CRC4 supports four-bit CRC on physical frames while no-CRC4 does not.

Example # Set the framing format on interface E1 2/0 to CRC4.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] frame-format crc4
```

idlecode (CE1/PRI interface view)

Syntax **idlecode** { **7e** | **ff** }

undo idlecode

View CE1/PRI interface view

Parameter **7e**: Sets line idle code to 0x7e.

ff: Sets line idle code to 0xff.

Description Use the **idlecode** command to set the line idle code on the CE1/PRI interface. Two types of line idle code are available: 0x7E and 0xFF.

Use the **undo idlecode** command to restore the default, that is, 0x7E.

The line idle code is sent in the timeslots that are not bundled into logical channels.

Example # Set the line idle code to 0x7E on CE1/PRI interface E1 2/0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] idlecode 7e
```

itf (CE1/PRI interface view)

Syntax **itf** { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **type** | **number** }

View CE1/PRI interface view

Parameter **number** *number*: Sets the number of interframe filling tags, which ranges from 0 to 14.

type { **7e** | **ff** }: Sets the type of interframe filling tag to 0x7E by specifying the **7e** argument or to 0xFF by specifying the **ff** keyword.

Description Use the **itf** command to set the type of and the number of interframe filling tags on the CE1/PRI interface. Two types of interframe filling tag are available: 0x7E and 0xFF.

Use the **undo itf** command to restore the default.

By default, interframe filling tag is 0x7E and the number of interframe filling tags is 4.

Interframe filling tags are sent when no service data is sent on the timeslots bundled into logical channels on the CE1/PRI interface.

Example # Set the type of interframe filling tag to 0xFF on CE1/PRI interface E1 2/0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] itf type ff
```

Set the number of interframe filling tags to five on CE1/PRI interface E1 2/0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] itf number 5
```

loopback (CE1/PRI interface view)

Syntax **loopback** { **local** | **payload** | **remote** }

undo loopback

View CE1/PRI interface view

Parameter **local**: Sets the interface in local loopback mode.

remote: Sets the interface in external loopback mode.

payload: Sets the interface in external payload loopback mode.

Description Use the **loopback** command to enable loopback and set the loopback mode.

Use the **undo loopback** command to restore the default.

By default, loopback is disabled.

Loopback is intended for checking the condition of interfaces or cables. Disable it otherwise.

You can bundle timeslots on the CE1/PRI interface to form a serial interface and encapsulate it with PPP. After you enable loopback on this serial interface, it is normal that the state of the link layer protocol is reported down.

Example # Set interface E1 2/0 in internal loopback mode.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] loopback local
```

pri-set (CE1/PRI interface view)

Syntax **pri-set** [**timeslot-list** *list*]

undo pri-set

View CE1/PRI interface view

Parameter **timeslot-list** *list*: Specifies timeslots to be bundled. The *list* argument is timeslot numbers, in the range of 1 to 31. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*.

Description Use the **pri-set** command to bundle timeslots on the CE1/PRI interface into a PRI set.

Use the **undo pri-set** command to remove the bundle.

By default, no PRI set is created.

On a CE1/PRI interface in PRI mode, timeslot 0 is used for frame synchronization control (FSC), timeslot 16 as the D channel for signaling transmission, and other timeslots as B channels for data transmission.

You can create only one PRI set on a CE1/PRI interface. This PRI set can include any timeslots except timeslot 0 and must include timeslot 16. Note that timeslot 16 cannot form a bundle that includes itself only. The attempt to bundle only timeslot 16 will fail.

If no timeslot is specified in this command, all timeslots except timeslot 0 are bundled into an interface in the form of 30B + D.

Upon creation of the PRI set, the system creates a serial interface logically equivalent to an ISDN PRI interface. The serial interface is named in the form of **serial** *number***:15**, where *number* represents the number of the CE1/PRI interface where the serial interface is created.

Because a channel set and a PRI set cannot coexist on a CE1/PRI interface, your PRI set creation attempt will fail if the **channel-set** command is configured.

Example # Bundle timeslots 1, 2, and 8 through 12 into a PRI set on CE1/PRI interface E1 2/0.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] pri-set timeslot-list 1,2,8-12
```

reset counters controller e1

Syntax **reset counters controller e1** *interface-number*

View User view

Parameter *interface-number*: Interface number.

Description Use the **reset counters controller e1** command to clear the controller counter for a CE1/PRI interface.

To display the information of the controller counter, use the **display controller e1** command.

- *The **reset counters interface** command does not clear the controller counters of CE1/PRI interfaces. To do that, use the **reset counters controller e1** command.*
- *The controller counters information that is cleared using the **reset counters controller e1** command is the same information that you can view with the **display controller e1** [interface-number] command.*

Example # Clear the controller counter for CE1/PRI interface E1 2/0.

```
<Sysname> reset counters controller e1 2/0
```

using (CE1/PRI interface view)

Syntax **using** { **ce1** | **e1** }

undo using

View CE1/PRI interface view

Parameter **ce1**: Sets the interface to operate in CE1/PRI mode.

e1: Sets the interface to operate in E1 mode.

Description Use the **using** command to configure the operating mode of the CE1/PRI interface.

Use the **undo using** command to restore the default, that is, CE1/PRI mode.

A CE1/PRI interface can work in either E1 mode (non-channelized mode) or CE1/PRI mode (channelized mode).

In E1 mode, the interface equals a 2 Mbps interface without timeslot division. Its logical features are the same like those of a synchronous serial interface. In CE1/PRI mode, it is physically divided into 32 timeslots numbered 0 through 31, where timeslot 0 is used for FSC. This interface can work as either a CE1 interface or a PRI interface.

After you set the CE1/PRI interface to work in E1 mode, the system automatically creates a serial interface numbered **serial** *interface-number***:0**, where *interface-number* represents the number of the CE1/PRI interface.

Example # Set CE1/PRI interface E1 2/0 to work in E1 mode.

```
<Sysname> system-view
[Sysname] controller e1 2/0
[Sysname-E1 2/0] using e1
```

13 FUNDAMENTAL CT1/PRI INTERFACE CONFIGURATION COMMANDS

alarm-threshold

Syntax **alarm-threshold** { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** | **pulse-recovery** } *value* }

undo alarm-threshold

View CT1/PRI interface view

Parameter **ais**: Sets the alarm threshold of alarm indication signal (AIS), which can be **level-1** and **level-2**.

- The **level-1** keyword specifies to generate an AIS alarm when the number of 0s in the bit stream of an SF or ESF frame is less than or equal to 2.
- The **level-2** keyword specifies to generate an AIS alarm when the number of 0s is less than or equal to 3 in the bit stream of an SF frame or less than or equal to 5 in the bit stream of an ESP frame.

By default, level-1 AIS alarm threshold applies.

lfa: Sets the loss of frame align (LFA) alarm threshold, which can be **level-1**, **level-2**, **level-3**, and **level-4**.

- The **level-1** keyword specifies to generate an LFA alarm when two of four frame alignment bits are lost.
- The **level-2** keyword specifies to generate an LFA alarm when two of five frame alignment bits are lost.
- The **level-3** keyword specifies to generate an LFA alarm when two of six frame alignment bits are lost.
- The **level-4** keyword applies only to ESF frames. It specifies to generate an LFA alarm when errors are detected in four consecutive ESF frames.

By default, level-1 LFA alarm threshold applies.

los: Sets a loss of signal (LOS) alarm threshold, which can be **pulse-detection** (for the pulse detection duration threshold with LOS) and **pulse-recovery** (for the pulse threshold with LOS).

The threshold of pulse-detection, in units of pulse intervals, ranges from 16 to 4,096 and defaults to 176.

The threshold of pulse-recovery, ranges from 1 to 256 and defaults to 22.

If the number of the pulses detected during the total length of the specified pulse detection intervals is smaller than the pulse-recovery threshold, a LOS alarm occurs. For example, if the two thresholds take their defaults, a LOS alarm is created if the number of pulses detected within 176 pulse intervals is less than 22.

Description Use the **alarm-threshold** command to set LOS, AIS, or LFA alarm thresholds on the CT1/PRI interface.

Use the **undo alarm-threshold** command to restore the defaults.

Example # Set the number of detection intervals to 300 for the pulse detection duration threshold.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] alarm-threshold los pulse-detection 300
```

bert (CT1/PRI interface view)

Syntax **bert pattern** { **2^15** | **2^20** } **time** *minutes* [**unframed**]

undo bert

View CT1/PRI interface view

Parameter **pattern**: Sets a bit error rate test (BERT) pattern, which could be 2^15 or 2^20.

2^15: Two to the fifteenth power, length of transmitted BERT pattern in bits.

2^20: Two to the twentieth power, length of transmitted BERT pattern in bits.

time *minutes*: Sets the duration (in minutes) of a BERT test. The *minutes* argument ranges from 1 to 1,440.

unframed: Sets the test pattern to cover the overhead bits of the frame.

Description Use the **bert** command to start a BERT test on a CT1/PRI interface.

Use the **undo bert** command to stop the BERT test running on the CT1/PRI interface.

ITU O.151, ITU O.153, and ANSI T1.403-1999 define many BERT patterns, among which, the CT1/PRI interface supports only 2^15 and 2^20 at present.

When running a BERT test, the local end sends out a pattern, which is to be looped over somewhere on the line and back to the local end. The local end then checks the received pattern for bit error rate, and by so doing helps you identify the condition of the line. To this end, you must configure loopback to allow the transmitted pattern to loop back from somewhere on the line, for example, from the far-end interface by placing the interface in a far-end loopback.

You may view the state and result of the BERT test with the **display controller t1** command.

Example # Run a 10-minute 2^20 BERT test on CT1/PRI interface t1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] bert pattern 2^20 time 10
```

cable (CT1/PRI interface view)

Syntax **cable** { **long** { **0db** | **-7.5db** | **-15db** | **-22.5db** } | **short** { **133ft** | **266ft** | **399ft** | **533ft** | **655ft** } }

undo cable

View CT1/PRI interface view

Parameter **long**: Matches 199.6-meter (655-feet) and longer cable length. The options for this parameter include **0db**, **-7.5db**, **-15db** and **-22.5db**. The attenuation parameter is selected depending on the signal quality received at the receiving end. In this case, no external CSU is needed.

short: Matches a cable length shorter than 199.6 meters (655 feet). The options for this parameter include **133ft**, **266ft**, **399ft**, **533ft** and **655ft**. The *length* parameter is selected depending on the actual transmission distance.

Description Use the **cable** command to set the cable attenuation and length on the CT1/PRI interface.

Use the **undo cable** command to restore the default, that is, **long 0db**.

You may use this command to adapt signal waveform to different transmission conditions such as the quality of the signal received by the receiver. If the signal quality is good, you can use the default setting. In this case, the CT1/PRI interface does not need an external CSU device.

Example # Set the cable length to 40.5 meter (133 feet) on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] cable short 133ft
```

channel-set (CT1/PRI interface view)

Syntax **channel-set** *set-number* **timeslot-list** *list* [**speed** { **56k** | **64k** }]

undo channel-set [*set-number*]

View CT1/PRI interface view

Parameter *set-number*: The number of the channel set formed by timeslot bundling on the interface. It ranges from 0 to 23.

timeslot-list *list*: Specifies timeslots to be bundled. The *list* argument is timeslot numbers, in the range of 1 to 24. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*.

speed { **56k** | **64k** }: Speed of the timeslot bundle (the channel set) in kbps. If **56k** is selected, the timeslots is bundled into N × 56 kbps bundles. If **64k**, the default, is selected, the timeslots is bundled into N × 64 kbps bundles.

Description Use the **channel-set** command to bundle timeslots on the CT1/PRI interface into a channel set.

Use the **undo channel-set** command to remove a specified or all channel sets.

By default, no timeslots are bundled into channel sets.

A CT1/PRI interface is physically divided into 24 timeslots numbered 1 through 24. In actual applications, all the timeslots can be bundled into multiple channel sets. For each channel set, the system automatically creates a serial interface logically equivalent to a synchronous serial interface.

The serial interface is named in the form of **serial** *interface-number:set-number*, where *interface-number* starts from the maximum serial interface number plus 1, and *set-number* represents the number of the channel set.

Only one timeslot bundling mode is supported on a CT1/PRI interface at a time. In other words, you cannot use this command together with the **pri-set** command.

Example # Bundle timeslots 1, 2, 5, 10 through 15, and 18 into channel set 0 on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] channel-set 0 timeslot-list 1,2,5,10-15,18
```

clock (CT1/PRI interface view)

Syntax **clock** { **master** | **slave** }

undo clock

View CT1/PRI interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **clock** command to configure clock source for the CT1/PRI interface.

Use the **undo clock** command to restore the default clock source, that is, line clock.

When the CT1/PRI interface is working as DCE, choose the internal clock for it. When it is working as DTE, choose the line clock for it.

Example # Use the internal clock as the clock source on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] clock master
```

code (CT1/PRI interface view)

Syntax **code** { **ami** | **b8zs** }

undo code

View CT1/PRI interface view

Parameter **ami**: Adopts AMI line code format.

b8zs: Adopts bipolar with 8-zero substitution (B8ZS) line code format.

Description Use the **code** command to set the line code format for the CT1/PRI interface.

Use the **undo code** command to restore the default, that is, B8ZS.

Keep the line code format of the interface in consistency with the one used on the remote device.

Example # Set the line code format of the interface T1 2/0 to AMI.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] code ami
```

controller t1

Syntax **controller t1** *number*

View System view

Parameter *number*: CT1/PRI interface number.

Description Use the **controller t1** command to enter CT1/PRI interface view.

Example # Enter the view of interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0]
```

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit CRC.

32: Adopts 32-bit CRC.

none: Disables CRC.

Description Use the **crc** command to configure CRC mode for a synchronous serial interface formed on a CE1/PRI interface.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

Example # Apply 32-bit CRC to a serial interface formed on interface CT1 interface 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] channel-set 1 timeslot-list 2-6
[Sysname-T1 2/0] quit
[Sysname] interface serial 2/0:1
[Sysname-Serial2/0:1] crc 32
```

data-coding (CT1/PRI interface view)

Syntax **data-coding** { **inverted** | **normal** }

undo data-coding

View CT1/PRI interface view

Parameter **inverted**: Enables user data inversion.

normal: Disables user data inversion.

Description Use the **data-coding normal** command to disable user data inversion on the CT1/PRI interface.

Use the **data-coding inverted** command to enable user data inversion on the CT1/PRI interface.

Use the **undo data-coding** command to restore the default.

By default, data inversion is disabled.

To prevent 7e in valid data from being taken for stuffing characters, HDLC inserts a zero after every five ones in the data stream. Then, HDLC inverts every one bit into a zero and every zero bit into a one. This ensures at least one out of every eight bits is a one. When AMI encoding is adopted on a T1 interface, the use of data inversion can eliminate the presence of multiple consecutive zeros.

At the two ends of the line, the same data inversion setting must be adopted.

Example # Enable user data inversion on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] data-coding inverted
```

display controller t1

Syntax **display controller t1** [*interface-number*]

View Any view

Parameter *interface-number*: Interface number. In conjunction with the **t1** keyword, it specifies a CT1/PRI interface.

Description Use the **display controller t1** command to display information about one specified or all CT1/PRI interfaces.

This command displays the following information about the specified interface:

- Physical state
- Cable type
- Framing
- Clock source (mode)
- Line code format
- Loopback mode
- Line idle code type
- Interframe filling tag type
- Alarm states
- Error statistics gathered at 15-minute intervals during the last 24 hours

Example # Display information about interface T1 2/0.

```
<Sysname> display controller t1 2/0
T1 2/0 current state :DOWN
Description : T1 2/0 Interface
Basic Configuration:
```

```
  Work mode is T1 framed, Cable type is 100 Ohm balanced.
  Frame-format is esf, fdl is none, Line code is b8zs.
  Source clock is slave, Data-coding is normal.
  Idle code is ff, Itf type is ff, Itf number is 2.
  Loop back is not set.
Alarm State:
  Receiver alarm state is Loss-of-Signal.
  Transmitter is sending remote alarm.
  Pulse density violation detected.
SendLoopCode History:
  inband-llb-up:0 times, inband-llb-down:0 times.
  fdl-ansi-llb-up:0 times, fdl-ansi-llb-down:0 times.
  fdl-ansi-plb-up:0 times, fdl-ansi-plb-down:0 times.
BERT state:(stopped, not completed)
  Test pattern: 2^15, Status: Not Sync, Sync Detected: 0
    Time: 0 minute(s), Time past: 0 minute(s)
    Bit Errors (since test started): 0 bits
    Bits Received (since test started): 0 Kbits
    Bit Errors (since latest sync): 0 bits
    Bits Received (since latest sync): 0 Kbits
Historical Statistics:
Last clearing of counters: Never
  Data in current interval (285 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 286 Los Alarm Secs
    7 Slip Secs, 286 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 286 Unavail Secs
  Data in Interval 1:
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 901 Los Alarm Secs
    22 Slip Secs, 901 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 901 Unavail Secs
  Data in Interval 2:
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 900 Los Alarm Secs
    23 Slip Secs, 900 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs
  Total Data (last 2 15 minute intervals):
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 2087 Los Alarm Secs
    52 Slip Secs, 2087 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2087 Unavail Secs
```

Table 18 Description on the fields of the display controller t1 command

Field	Description
T1 2/0/0 current state	Physical state of the interface: up or down
Description	Description about the T1 interface
Basic Configuration	Basic configurations of the interface
Work mode	Operating mode of the T1 interface, T1 framed in this example
Cable type	Cable type of the T1 interface, 100 ohm balanced in this example
Frame-format	Frame format configured on the T1 interface: ESF or SF
fdl	FDL format: ANSI, ATT, or none
Line code	Line code: AMI or B8ZS
Source clock	Source clock used by the interface: master for the internal clock or slave for the line clock
Data-coding	Normal or inverted
Idle code	0x7E or 0xFF
Itf type	Type of interframe filling tag: 0x7E or 0xFF

Table 18 Description on the fields of the display controller t1 command

Field	Description
Itf number	Number of interframe filling tags
Loop back	Loopback setting on the interface: local, payload, remote, or not set
Alarm State	Alarm state
Receiver alarm state	Type of received alarm: none, LOS, LOF, RAI, or AIS
Transmitter is sending remote alarm.	Type of transmitted alarm: RAI, or none
Pulse density violation detected	The detected pulse density is incompliant with the specification
SendLoopCode History: inband-llb-up:0 times, inband-llb-down:0 times. fdl-ansi-llb-up:0 times, fdl-ansi-llb-down:0 times. fdl-ansi-plb-up:0 times, fdl-ansi-plb-down:0 times	History of loopback code sending to the far-end, including the number of transmissions for each type of code, and the type of the last sent code. (See "sendloopcode" on page 229.)
BERT state:(stopped, not completed)	BERT state: completed, stopped (not completed), or running.
Test pattern: 2^15, Status: Not Sync, Sync Detected: 0	Test pattern in use (2^20 or 2^15), 2^15 in this example; synchronization state, and the number of detected synchronizations
Time: 0 minute(s), Time past: 0 minute(s)	The duration of the BERT test and the time that has elapsed
Bit Errors (since test started)	Number of bit errors received since the start of the BERT test
Bits Received (since test started)	Number of bits received since the start of the BERT test
Bit Errors (since latest sync)	Number of bit errors received since the last synchronization
Bits Received (since latest sync)	Number of bits received since last synchronization
Historical Statistics:	Historical statistics
Last clearing of counters	Counter clearing records
Data in current interval (285 seconds elapsed): 0 Line Code Violations, 0 Path Code Violations 0 Ais Alarm Secs, 286 Los Alarm Secs 7 Slip Secs, 286 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 286 Unavail Secs	Statistics spanning the current interval. The statistical items, such as AIS alarm, LOS signal, and LFA, are provided according to the T1 specifications for the physical layer. For details, refer to ANSI T1.403 and AT&T TR 54016.

Table 18 Description on the fields of the display controller t1 command

Field	Description
Data in Interval 1:	Statistics spanning the first interval.
0 Line Code Violations, 0 Path Code Violations	The statistical items are the same as those provided by the statistics spanning the current interval.
0 Ais Alarm Secs, 901 Los Alarm Secs	
22 Slip Secs, 901 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins	
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 901 Unavail Secs	
Data in Interval 2:	Statistics spanning the second interval.
0 Line Code Violations, 0 Path Code Violations	The statistical items are the same as those provided by the statistics spanning the current interval.
0 Ais Alarm Secs, 900 Los Alarm Secs	
23 Slip Secs, 900 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins	
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs	
Total Data (last 2 15 minute intervals):	Statistics spanning the last two intervals.
0 Line Code Violations, 0 Path Code Violations	The statistical items are the same as those provided by the statistics spanning the current interval.
0 Ais Alarm Secs, 2087 Los Alarm Secs	
52 Slip Secs, 2087 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins	
0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2087 Unavail Secs	

error-diffusion restraint config

Syntax **error-diffusion restraint config** *detect-timer renew-timer threshold*

undo error-diffusion restraint config

View System view

Parameter *detect-timer*: Setting of the error packet detect timer, in the range 30 to 600 (in seconds).

renew-timer: Setting of the renew timer, in the range 120 to 2400 (in seconds).

threshold: Error packet ratio threshold, in the range 5 to 100 (in percentage).

Description Use the **error-diffusion restraint config** command to set the three parameters in error packet diffusion restraint.

Use the **undo error-diffusion restraint enable** command to restore the default settings of the three parameters.

By default, the error packet detect timer is set to 30 seconds, the renew timer is set to 600 seconds, and the error packet ratio threshold is 20.

The setting of renew timer must be at least four times that of the error packet detect timer. If the total number of the packets received during *detect-timer* is less than 100, error packets are not counted.

- *The support for these two commands varies with device models.*
- *These two commands apply to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # Set the error packet detect timer to 100 seconds, the renew timer to 2400 seconds, and the error packet ratio threshold to 15.

```
<Sysname> system-view
[Sysname] error-diffusion restraint config 100 2400 15
```

error-diffusion restraint enable

Syntax **error-diffusion restraint enable**

undo error-diffusion restraint enable

View System view

Parameter None

Description Use the **error-diffusion restraint enable** command to enable error packet diffusion restraint.

Use the **undo error-diffusion restraint enable** command to disable error packet diffusion restraint.

By default, the function is disabled.

- *The support of these two commands varies with device model.*
- *These two commands apply to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # Enable error packet diffusion restraint.

```
<Sysname> system-view
[Sysname] error-diffusion restraint enable
```

error-diffusion restraint restart-channel

Syntax **error-diffusion restraint restart-channel serial** *interface-number*:*set-number*

View System view

Parameter **serial** *interface-number:set-number*: Specifies a channel formed on a CE1/PRI interface. The *interface-number* argument is a CE1/PRI interface number, and the *set-number* argument is a channel set number.

Description Use the **error-diffusion restraint restart-channel** command to bring up a channel previously shut down by the error packet diffusion restraint function.

- *The support of this command varies with device model.*
- *This command applies to CT1/PRI interfaces and CE1/PRI interfaces only.*

Example # Bring up channel Serial 2/0:0 (assuming that the channel is shut down by the error packet diffusion restraint function).

```
<Sysname> system-view
[Sysname] error-diffusion restraint restart-channel serial 2/0:0
```

fdl

Syntax **fdl** { **ansi** | **att** | **none** }

undo fdl

View CT1/PRI interface view

Parameter **ansi**: Implements ANSI T1.403 FDL.

att: Implements AT&T TR 54016 FDL.

none: Disables facilities data link (FDL).

Description Use the **fdl** command to set the behavior of the CT1/PRI interface on the FDL in ESF framing.

Use the **undo fdl** command to restore the default.

By default, FDL is disabled (none).

FDL is an embedded 4 kbps overhead channel within the ESF format for transmitting performance statistics or loopback code.

Example # Implement AT&T TR 54016 FDL on interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] fdl att
```

frame-format (CT1/PRI interface view)

Syntax **frame-format** { **esf** | **sf** }

undo frame-format

View CT1/PRI interface view

Parameter **sf**: Sets the framing format to super frame (SF).

esf: Sets the framing format to extended super frame (ESF).

Description Use the **frame-format** command to set the framing format on the CT1/PRI interface.

Use the **undo frame-format** command to restore the default, that is, **esf**.

CT1/PRI interfaces support two framing formats, that is, SF and ESF. In SF format, multiple frames can share the same FSC and signaling information, so that more significant bits are available for transmitting user data. The use of ESF allows you to test the system without affecting the ongoing service.

Example # Set the framing format of interface T1 2/0 to SF.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] frame-format sf
```

idlecode (CT1/PRI interface view)

Syntax **idlecode** { **7e** | **ff** }

undo idlecode

View CT1/PRI interface view

Parameter **7e**: Sets the line idle code to 0x7E.

ff: Sets the line idle code to 0xFF.

Description Use the **idlecode** command to set the line idle code on the CT1/PRI interface. Two types of line idle code are available: 0x7E and 0xFF.

Use the **undo idlecode** command to restore the default, that is, 0x7E.

The line idle code is sent in the timeslots that are not bundled into the logical channels on the interface.

Example # Set the line idle code to 0x7E on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] idlecode 7e
```

itf (CT1/PRI interface view)

Syntax **itf** { **number** *number* | **type** { **7e** | **ff** } }

undo itf { **number** | **type** }

View CT1/PRI interface view

Parameter **number** *number*: Sets the number of interframe filling tags (an interframe filling tag is one byte in length). The *number* argument ranges from 0 to 14.

type { **7e** | **ff** }: Sets the interframe filling tag to 0x7E by specifying the **7e** keyword or to 0xFF by specifying the **ff** keyword. On CT1/PRI interfaces, the default interframe filling tag is 0x7E.

Description Use the **itf** command to set the type and the number of interframe filling tags on the CT1/PRI interface. Two types of interframe filling tag are available: 0x7E and 0xFF.

Use the **undo itf** command to restore the default.

By default, the interframe filling tag is 0x7E, the number of interframe filling tags is 4.

Interframe filling tags are sent when no service data is sent on the timeslots bundled into logical channels on a CT1/PRI interface.

Example # Set the interframe filling tag to 0xFF on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] itf type ff
```

Set the number of interframe filling tags to five on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] itf number 5
```

loopback (CT1/PRI interface view)

Syntax **loopback** { **local** | **payload** | **remote** }

undo loopback

View CT1/PRI interface view

Parameter **local**: Enables the CT1/PRI interface to perform local loopback.

payload: Enables the interface to perform external payload loopback.

remote: Enables the interface to perform remote loopback.

Description Use the **loopback** command to enable local, remote, or external payload loopback on the CT1/PRI interface.

Use the **undo loopback** command to restore the default.

By default, loopback is disabled.

Loopback is intended for checking the condition of interfaces or cables. Disable it otherwise.

You can bundle timeslots on a CT1/PRI interface to form a serial interface and encapsulate it with PPP. After you enable loopback on this serial interface, it is normal that the state of the link layer protocol is reported down.

Example # Enabled remote loopback on interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] loopback remote
```

pri-set (CT1/PRI interface view)

Syntax **pri-set** [**timeslot-list** *list*]

undo pri-set

View CT1/PRI interface view

Parameter *list*: Specifies timeslots to be bundled. Timeslots are numbered 1 through 24. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1***-***number2*, or several discrete timeslots by specifying *number1*, *number2***-***number3*.

Description Use the **pri-set** command to bundle timeslots into a PRI set on the CT1/PRI interface.

Use the **undo pri-set** command to remove the timeslot bundle.

By default, no PRI set is created.

When creating a PRI set on a CT1/PRI interface, note that timeslot 24 is the D channel for transmitting signaling; it cannot form a bundle that includes itself only. The attempts to bundle only timeslot 24 will fail.

In the created PRI set, timeslot 24 is used as D channel for signaling transmission, and the other timeslots as B channels for data transmission. You may randomly bundle these timeslots into a PRI set (as the D channel, timeslot 24 is automatically bundled). If no timeslot is specified, all timeslots are bundled into an interface similar to an ISDN PRI interface in the form of 23B+D.

For the PRI set, the system automatically creates a serial interface logically equivalent to an ISDN PRI interface. The serial interface is named in the form of **serial** *number***:23**, where *number* is the number of the CT1/PRI interface on which the serial interface is created.

Because a channel set and a PRI set cannot coexist on a CT1/PRI interface, your PRI set creation attempt will fail if the **channel-set** command is configured.

Example # Bundle timeslots 1, 2, and 8 through 12 into a PRI set on CT1/PRI interface T1 2/0.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] pri-set timeslot-list 1,2,8-12
```

reset counters controller t1

Syntax **reset counters controller t1** *interface-number*

View User view

Parameter *interface-number*: Interface number.

Description Use the **reset counters controller t1** command to clear the controller counter for a CT1/PRI interface.

To display the value of the controller counter, use the **display controller t1** command.

*The **reset counters interface** command cannot clear the controller counters for CT1/PRI interfaces. To do so, you must use the **reset counters controller t1** command.*

Example # Clear the controller counter for CT1/PRI interface T1 2/0.

```
<Sysname> reset counters controller t1 2/0
```

sendloopcode

Syntax **sendloopcode** { **fdl-ansi-llb-down** | **fdl-ansi-llb-up** | **fdl-ansi-plb-down** | **fdl-ansi-plb-up** | **fdl-att-plb-down** | **fdl-att-plb-up** | **inband-llb-down** | **inband-llb-up** }

View CT1/PRI interface view

Parameter **fdl-ansi-llb-down**: Sends ANSI-compliant LLB deactivation request code in the FDL to remove loopback.

fdl-ansi-llb-up: Sends ANSI-compliant line loopback (LLB) activation request code in the FDL to start remote loopback.

fdl-ansi-plb-down: Sends ANSI-compliant PLB deactivation request code in the FDL to remove loopback.

fdl-ansi-plb-up: Sends ANSI-compliant payload loopback (PLB) activation request code in the FDL to start remote loopback.

fdl-att-plb-down: Sends AT&T-complaint PLB deactivation request code in the FDL to remove loopback.

fdl-att-plb-up: Sends AT&T-complaint PLB activation request code in the FDL to start remote loopback.

inband-llb-down: Sends in-band LLB deactivation request code compliant with the ANSI or AT&T implementation to remove loopback.

inband-llb-up: Sends in-band line loopback (LLB) activation request code compliant with the ANSI and AT&T implementation to start remote loopback.

Description Use the **sendloopcode** command to send remote loopback control code.

By default, no remote loopback control code is sent.

You may configure loopback on the far-end CT1/PRI interface by sending loopback request code.

In LLB mode, all 193 bits (one synchronization bit and 192 effective bandwidth bits) in a T1 PCM frame are looped back. In PLB mode, however, only 192 effective bandwidth bits are looped back.

The format of loopback code can be compliant with ANSI T1.403 or AT&T TR 54016.

In SF framing, LLB code is sent using the effective bandwidth. In ESF framing, both LLB code and PLB code are sent/received in the FDL.

Use this command in conjunction with the far-end T1 device. The far-end device must be able to set loopback mode depending on the detected loopback code.

The sending of remote loopback control code lasts five minutes without affecting the operation of other interfaces.

Example # Send in-band LLB activation request code.

```
<Sysname> system-view
[Sysname] controller t1 2/0
[Sysname-T1 2/0] sendloopcode inband-llb-up
```

14 E1-F INTERFACE CONFIGURATION COMMANDS

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit CRC.

32: Adopts 32-bit CRC.

none: Disables CRC.

Description Use the **crc** command to configure CRC mode for an E1-F interface.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

Example # Adopt 32-bit CRC on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] crc 32
```

display fe1

Syntax **display fe1** [**serial** *interface-number*]

View Any view

Parameter **serial** *interface-number*: Specifies a serial interface. If no interface is specified, information on all the E1-F interfaces is displayed.

Description Use the **display fe1 serial** command to display the configuration and state information about the specified or all E1-F interfaces.

If the specified interface is a common serial interface rather than an E1-F interface, the system will display the prompt.

Example # Display the information about an E1-F interface.

```
<Sysname> display fe1 serial 2/0
 Serial2/0
 Basic Configuration:
    E1 FRAMED
Physical type is  FE1 - 75 OHM unbalanced
    Frame-format is  NONE,Line Code is HDB3,Source Clock is SLAVE
  Alarm State:
    Receiver alarm state is None.
Historical Statistics:
Last clearing of counters: Never
    Data in current interval (19349 seconds elapsed):
    129 Loss Frame Alignment Secs, 0 Framing Error Secs,
    0 CRC Error Secs, 0 Alarm Indication Secs, 129 Loss-of-signals Secs,
    0 Code Violations Secs, 0 Slip Secs, 0 E-Bit error Secs.
```

Table 19 Description on the fields of the display fe1 serial command

Field	Description
E1 FRAMED	Operating mode, framed or unframed. In this sample output, it is framed
Physical type	Interface type (75-ohm unbalanced/120-ohm balanced)
Frame-format	Framing format (CRC4/no-CRC4)
Line Code	Line code format: AMI or HDB3.
Source Clock	Source clock: master for internal clock and slave for line clock
Alarm State	Alarm information

fe1 cable

Syntax **fe1 cable** { **long** | **short** }

undo fe1 cable

View E1-F interface view

Parameter **long**: Supports long-haul cables.

short: Supports short-haul cables.

Description Use the **cable** command to set the cable length for an E1-F interface.

Use the **undo cable** command to restore the default.

By default, the **long** keyword applies.

Example # Set the cable length type on E1-F interface Serial 2/0 to short.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 cable short
```

fe1 clock

Syntax **fe1 clock** { **master** | **slave** }

undo fe1 clock

View E1-F interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **fe1 clock** command to configure clock source for the E1-F interface.

Use the **undo fe1 clock** command to restore the default, that is, line clock.

When the E1-F interface is working as DCE, choose the internal clock (**master**) for it. When it is working as DTE, choose the line clock for it.

Example # Use the internal clock as the clock source on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 clock master
```

fe1 code

Syntax **fe1 code** { **ami** | **hdb3** }

undo fe1 code

View E1-F interface view

Parameter **ami**: Adopts AMI line code format.

hdb3: Adopts HDB3 line code format.

Description Use the **fe1 code** command to set the line code format for the E1-F interface.

Use the **undo fe1 code** command to restore the default, that is, HDB3.

Keep the line code format of the interface in consistency with that used by the remote device.

Example # Set the line code format of interface Serial 2/0 to AMI.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 code ami
```

fe1 detect-ais

Syntax **fe1 detect-ais**

undo fe1 detect-ais

View E1-F interface view

Parameter None

Description Use the **fe1 detect-ais** command to enable AIS test on an interface.

Use the **undo fe1 detect-ais** command to disable AIS test.

By default, AIS test is performed.

Example # Enable AIS test on E1-F 2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 detect-ais
```

fe1 frame-format

Syntax **fe1 frame-format** { **crc4** | **no-crc4** }

undo fe1 frame-format

View E1-F interface view

Parameter **crc4**: Sets framing format to CRC4.

no-crc4: Sets framing format to no-CRC4.

Description Use the **fe1 frame-format** command to configure the framing format of the E1-F interface.

Use the **undo fe1 frame-format** command to restore the default, that is, no-CRC4.

An E1-F interface in framed mode supports both CRC4 and no-CRC4 framing formats, where CRC4 supports four-bit CRC on physical frames while no-CRC4 does not.

Example # Set the framing format of E1-F interface Serial 2/0 to CRC4.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 frame-format crc4
```

fe1 loopback

Syntax **fe1 loopback** { **local** | **payload** | **remote** }

undo fe1 loopback

View E1-F interface view

Parameter **local**: Sets the interface in internal loopback mode.

payload: Sets the interface in external payload loopback mode.

remote: Sets the interface in external loopback mode.

Description Use the **fe1 loopback** command to set the E1-F interface in a loopback mode.

Use the **undo fe1 loopback** command to restore the default.

By default, loopback is disabled.

Loopback is intended for checking the condition of interfaces or cables. Disable it otherwise.

The three loopback modes cannot be used at the same time on an E1-F interface.

Example # Set interface Serial 2/0 in internal loopback mode.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 loopback local
```

fe1 timeslot-list

Syntax **fe1 timeslot-list** *list*

undo fe1 timeslot-list

View E1-F interface view

Parameter *list*: Specifies timeslots to be bundled. They are numbered 1 through 31. You may specify a single timeslot by specifying its number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*.

Description Use the **fe1 timeslot-list** command to bundle timeslots on the E1-F interface.

Use the **undo fe1 timeslot-list** command to restore the default.

By default, all the timeslots on the E1-F interface are bundled to form a 1984 kbps interface.

Timeslot bundling results in interface rate change. For example, after you bundle timeslots 1 through 10 on the interface, the interface rate becomes 10 × 64 kbps.

Only one channel set can be created on an E1-F interface, and this channel set is associated with the current synchronous serial interface. On a CE1/PRI interface, however, you may create multiple channel sets; for each of them, the system automatically creates a synchronous serial interface.

Timeslot 0 on E1-F interfaces is used for synchronization. Therefore, a bundling operation only involves timeslots 1 through 31.

When the E1-F interface is working in unframed mode, the **fe1 timeslot-list** command is invalid.

Related command: **fe1 unframed**.

Example # Bundle timeslots 1, 2, 5, 10 through 15, and 18 on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0]fe1 timeslot-list 1,2,5,10-15,18
```

fe1 idlecode

Syntax **fe1 idlecode** { **7e** | **ff** }

undo fe1 idlecode

View E1-F interface view

Parameter **7e**: Sets the line idle code to 0x7E.

ff: Sets the line idle code to 0xFF.

Description Use the **fe1 idlecode** command to set the line idle code on the E1-F interface. Two types of line idle code are available: 0x7E and 0xFF.

Use the **undo fe1 idlecode** command to restore the default, that is, 0x7E.

The line idle code is sent in the timeslots that are not bundled into the logical channels on the interface.

Example # Set the line idle code to 0x7E on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 idlecode 7e
```

fe1 itf

Syntax **fe1 itf** { **number** *number* | **type** { **7e** | **ff** } }

undo fe1 itf { **number** | **type** }

View E1-F interface view

Parameter **number** *number*: Sets the number of interframe filling tags (an interframe filling tag is one byte in length). The *number* argument ranges from 0 to 14.

type { **7e** | **ff** }: Sets the type of interframe filling tag to 0x7E by specifying the **7e** keyword or to 0xFF by specifying the **ff** keyword. The default is 0x7E.

Description Use the **fe1 itf** command to set the type of and the number of interframe filling tags on the E1-F interface. Two types of interframe filling tag are available: 0x7E and 0xFF.

Use the **undo itf** command to restore the default.

By default, the interframe filling tag is 0x7E and the number of interframe filling tags is 4.

Interframe filling tags are sent when no service data is sent on the timeslots bundled into the logical channel on the E1-F interface.

Example # Set the type of interframe filling tag to 0xFF on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 itf type ff
```

Set the number of interframe filling tags to five on E1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 itf number 5
```

fe1 unframed

Syntax **fe1 unframed**

undo fe1 unframed

View E1-F interface view

Parameter None

Description Use the **fe1 unframed** command to configure the E1-F interface to work in unframed mode.

Use the **undo fe1 unframed** command to configure the E1-F interface to work in framed mode.

By default, the E1-F interface works in framed mode.

When the E1-F interface is working in unframed mode, it is a 2048 kbps interface without timeslot division and is logically equivalent to a synchronous serial interface.

When it works in framed mode, it is physically divided into 32 timeslots numbered 0 through 31, where timeslot 0 is used for synchronization.

Related command: **fe1 timeslot-list**.

Example # Set E1-F interface Serial 2/0 to work in unframed mode.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fe1 unframed
```

15 T1-F INTERFACE CONFIGURATION COMMANDS

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit CRC.

32: Adopts 32-bit CRC.

none: Disables CRC.

Description Use the **crc** command to configure CRC mode for an T1-F interface.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

Example # Adopt 32-bit CRC on T1-F interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] crc 32
```

display ft1

Syntax **display ft1** [**serial** *interface-number*]

View Any view

Parameter **serial** *interface-number*: Specifies a serial interface. If no interface is specified, the information on all the T1-F interfaces is displayed.

Description Use the **display ft1 serial** command to display the configuration and state information about a T1-F interface.

If the specified interface is a common serial interface rather than a T1-F interface, the system will display the prompt.

Example # Display information about T1-F interface Serial 2/0.

```
<Sysname> display ft1 serial 2/0
Serial2/0
Input: 0 packets, 0 bytes
           0 broadcasts, 0 multicasts
           0 errors, 0 runts, 0 giants
           0 CRC, 0 align errors, 0 overruns
           0 dribbles, 0 aborts, 0 no buffers
           0 frame errors
    Output:0 packets, 0 bytes
           0 errors, 0 underruns, 0 collisions
           0 deferred
Basic Configuration:
  Work mode is T1 framed, Cable type is 100 Ohm balanced.
  Frame-format is esf, fdl is none, Line code is b8zs.
  Source clock is slave, Data-coding is normal.
  Idle code is ff, Itf type is ff, Itf number is 2
  Loop back is not set.
Alarm State:
  Receiver alarm state is Loss-of-Signal.
  Transmitter is sending remote alarm.
  Pulse density violation detected.
SendLoopCode History:
  inband-llb-up:0 times, inband-llb-down:0 times.
  fdl-ansi-llb-up:0 times, fdl-ansi-llb-down:0 times.
  fdl-ansi-plb-up:0 times, fdl-ansi-plb-down:0 times.
BERT state:(stopped, not completed)
  Test pattern: 2^15, Status: Not Sync, Sync Detected: 0
    Time: 0 minute(s), Time past: 0 minute(s)
    Bit Errors (since test started): 0 bits
    Bits Received (since test started): 0 Kbits
    Bit Errors (since latest sync): 0 bits
    Bits Received (since latest sync): 0 Kbits
Historical Statistics:
Last clearing of counters: Never
  Data in current interval (285 seconds elapsed):
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 286 Los Alarm Secs
    7 Slip Secs, 286 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 286 Unavail Secs
  Data in Interval 1:
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 901 Los Alarm Secs
    22 Slip Secs, 901 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 901 Unavail Secs
  Data in Interval 2:
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 900 Los Alarm Secs
    23 Slip Secs, 900 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs
  Total Data (last 2 15 minute intervals):
    0 Line Code Violations, 0 Path Code Violations
    0 Ais Alarm Secs, 2087 Los Alarm Secs
    52 Slip Secs, 2087 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins
    0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2087 Unavail Secs
```

Table 20 Description on the fields of the display ft1 serial command

Field	Description
Serial2/0	Interface type and number
Basic Configuration	Basic configurations for the interface
Input	Statistics about the input and output
Output	
Work mode	T1 interface operating mode, T1 framed in this sample output

Table 20 Description on the fields of the display ft1 serial command

Field	Description
Cable type	Cable type of the interface, 100 ohm balanced in this sample output
Frame-format	Frame format configured on the interface: ESF or SF
fdl	FDL format: ANSI, ATT, or none
Line code	AMI or B8ZS
Source Clock	Source clock used by the interface: master for the internal clock or slave for the line clock
Data-coding	Normal or inverted
Idle code	7e or ff
Itf type	Type of interframe filling tag: 7e or ff
Itf number	Number of interframe filling tags
Loop back	Loopback setting on the interface: local, payload, remote, or not set
Alarm State	Alarm state
Receiver alarm state	Type of received alarm: none, LOS, LOF, RAI, or AIS
Transmitter is sending remote alarm.	Type of transmitted alarm: RAI, or none
Pulse density violation detected	The detected pulse density is incompliant with the specification
SendLoopCode History: inband-llb-up:0 times, inband-llb-down:0 times. fdl-ansi-llb-up:0 times, fdl-ansi-llb-down:0 times. fdl-ansi-plb-up:0 times, fdl-ansi-plb-down:0 times	History of loopback code sending to the far-end, including the number of transmissions for each type of code, and the type of the last sent code. (See "ft1 sendloopcode" on page 251.)
BERT state:(stopped, not completed)	BERT state: completed, stopped (administratively stopped), or running.
Test pattern: 2^15, Status: Not Sync, Sync Detected: 0	Test pattern in use, 2^15 in this sample output; synchronization state, and the number of detected synchronizations
Time: 0 minute(s), Time past: 0 minute(s)	The duration of the BERT test and the time that has elapsed
Bit Errors (since test started)	Number of bit errors received since the start of the BERT test
Bits Received (since test started)	Number of bits received since the start of the BERT test
Bit Errors (since latest sync)	Number of bit errors received since the last synchronization
Bits Received (since latest sync)	Number of bits received since last synchronization
Historical Statistics:	Historical statistics
Last clearing of counters: Never	Counter clearing records

Table 20 Description on the fields of the display ft1 serial command

Field	Description
Data in current interval (285 seconds elapsed): 0 Line Code Violations, 0 Path Code Violations 0 Ais Alarm Secs, 286 Los Alarm Secs 7 Slip Secs, 286 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 286 Unavail Secs	Statistics spanning the current interval. The statistical items, such as AIS alarm, LOS signal, and LFA, are provided according to the T1 specifications for the physical layer. For details, refer to ANSI T1.403 and AT&T TR 54016.
Data in Interval 1: 0 Line Code Violations, 0 Path Code Violations 0 Ais Alarm Secs, 901 Los Alarm Secs 22 Slip Secs, 901 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 901 Unavail Secs	Statistics spanning the first interval. The statistical items are the same as those provided by the statistics spanning the current interval.
Data in Interval 2: 0 Line Code Violations, 0 Path Code Violations 0 Ais Alarm Secs, 900 Los Alarm Secs 23 Slip Secs, 900 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 900 Unavail Secs	Statistics spanning the second interval. The statistical items are the same as those provided by the statistics spanning the current interval.
Total Data (last 2 15 minute intervals): 0 Line Code Violations, 0 Path Code Violations 0 Ais Alarm Secs, 2087 Los Alarm Secs 52 Slip Secs, 2087 Fr Loss Secs, 0 Line Err Secs, 0 Degraded Mins 0 Errored Secs, 0 Bursty Err Secs, 0 Severely Err Secs, 2087 Unavail Secs	Statistics spanning the last two intervals. The statistical items are the same as those provided by the statistics spanning the current interval.

ft1 bert (T1-F interface view)

Syntax **ft1 bert pattern** { **2^15** | **2^20** } **time** *minutes* [**unframed**]

undo ft1 bert

View T1-F interface view

Parameter **pattern**: Sets a bit error rate test (BERT) pattern, which could be 2^15 or 2^20.

2^15: Two to the fifteenth power, length of transmitted BERT pattern in bits.

2^20: Two to the twentieth power, length of transmitted BERT pattern in bits.

time *minutes*: Sets the duration (in minutes) of a BERT test. The *minute* argument is up to 1,440.

unframed: Sets the test pattern to cover the overhead bits of the frame.

Description Use the **ft1 bert** command to start a BERT test on a T1-F interface.

Use the **undo ft1 bert** command to stop the BERT test running on the T1-F interface.

ITU O.151, ITU O.153, and ANSI T1.403-1999 define many BERT patterns, among which, the T1-F interface supports only 2^15 and 2^20 at present.

When running a BERT test, the local end sends out a pattern, which is to be looped over somewhere on the line and back to the local end. The local end then checks the received pattern for bit error rate, and by so doing helps you identify the condition of the line. To this end, you must configure loopback to allow the transmitted pattern to loop back from somewhere on the line, for example, from the far-end interface by placing the interface in a far-end loopback.

You may view the state and result of the BERT test with the **display ft1 serial** command.

Example # Run a 10-minute 2^20 BERT test on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 bert pattern 2^20 time 10
```

ft1 cable

Syntax **ft1 cable** { **long** *decibel* | **short** *length* }

undo ft1 cable

View T1-F interface view

Parameter **long** *decibel*: Matches 199.6-meter (655-feet) and longer cable length. The argument *decibel* can take **0db**, **-7.5db**, **-15db**, or **-22.5db**, depending on the signal quality at the receiving end. In this case, no external CSU is required.

short *length*: Matches a cable length shorter than 199.6 meters (655 feet). The argument *length* can take **133ft**, **266ft**, **399ft**, **533ft**, or **655ft**, depending on the actual transmission distance.

Description Use the **ft1 cable** command to set the cable attenuation and length on the T1-F interface.

Use the **undo ft1cable** command to restore the default, that is, **long 0db**.

You may use this command to adapt signal waveform to different transmission conditions such as the quality of the signal received by the receiver. If the signal quality is good, you can just use the default setting.

Example # Set the cable length to 40.5 meters (133 feet) on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0]ft1 cable short 133ft
```

ft1 clock

Syntax **ft1 clock** { **master** | **slave** }

undo ft1 clock

View T1-F interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **ft1 clock** command to configure the clock source for the T1-F interface.

Use the **undo ft1 clock** command to restore the default, that is, line clock.

When the T1-F interface is working as DCE, choose the internal clock for it. When it is working as DTE, choose the line clock for it.

When the T1-F interfaces on two routers are directly connected, one interface must work in master clock mode to provide the clock source while the other in slave clock mode to accept.

When the T1-F interface on your router is connected to an exchange, it is working as DTE and therefore must be configured with the slave clock mode to accept the line clock provided by the exchange working as DCE.

Example # Use the internal clock as the clock source on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 clock master
```

ft1 code

Syntax **ft1 code** { **ami** | **b8zs** }

undo ft1 code

View T1-F interface view

Parameter **ami**: Adopts AMI line code format.

b8zs: Adopts B8ZS line code format.

Description Use the **ft1 code** command to set the line code format for the T1-F interface.

Use the **undo ft1 code** command to restore the default, that is, B8ZS.

Keep the line code format of the interface in consistency with the one used on the remote device.

Example # Set the line code format of T1-F interface Serial 2/0 to AMI.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 code ami
```

ft1 data-coding

Syntax **ft1 data-coding** { **inverted** | **normal** }

undo ft1 data-coding

View T1-F interface view

Parameter **inverted**: Enables user data inversion.

normal: Disables user data inversion.

Description Use the **ft1 data-coding normal** command to disable user data inversion for a T1-F interface.

Use the **ft1 data-coding inverted** command to enable user data inversion for a T1-F interface.

Use the **undo ft1 data-coding** command to restore the default.

By default, data inversion is disabled.

To prevent 7e in valid data from being taken for stuffing characters, HDLC inserts a zero after every five ones in the data stream. Then, HDLC inverts every one bit into a zero and every zero bit into a one. This ensures at least at least one out of every eight bits is a one. When AMI encoding is adopted on a T1-F interface, the use of data inversion can eliminate presence of multiple consecutive zeros.

At the two ends of a T1-F line, the same data inversion setting must be adopted.

Example # Enable user data inversion on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 data-coding inverted
```

ft1 fdl

Syntax **ft1 fdl** { **ansi** | **att** | **both** | **none** }

undo ft1 fdl

View T1-F interface view

Parameter **ansi**: Adopts ANSI T1.403 for FDL.

att: Adopts AT&T TR 54016 for FDL.

both: Adopts both ANSI T1.403 and AT&T TR 54016 for FDL.

none: Disables FDL.

Description Use the **ft1 fdl** command to set the behavior of the T1-F interface on the FDL in ESF framing.

Use the **undo ft1 fdl** command to restore the default.

By default, FDL is disabled.

FDL is an embedded 4 kbps overhead channel within the ESF format for transmitting performance statistics or loopback code.

You can however change the setting depending on the setting at the far end.

Example # Implement ANSI T1.403 FDL on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 fdl ansi
```

ft1 frame-format

Syntax **ft1 frame-format** { **esf** | **sf** }

undo ft1 frame-format

View T1-F interface view

Parameter **esf**: Sets the framing format on the T1-F interface to ESF.

sf: Sets the framing format on the T1-F interface to SF.

Description Use the **frame-format** command to set the framing format on the T1-F interface.

Use the **undo frame-format** command to restore the default, that is, **esf**.

T1-F interfaces support two framing formats, that is, SF and ESF. In SF format, multiple frames can share the same FSC and signaling information, so that more significant bits are available for transmitting user data. The use of ESF allows you to test the system without affecting the ongoing service.

Example # Set the framing format of T1-F interface Serial 2/0 to SF.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 frame-format sf
```

ft1 idlecode

Syntax **ft1 idlecode** { **7e** | **ff** }

undo ft1 idlecode

View T1-F interface view

Parameter **7e**: Sets the line idle code to 0x7E.

ff: Sets the line idle code to 0xFF.

Description Use the **ft1 idlecode** command to set the line idle code on the T1-F interface. Two types of line idle code are available: 0x7E and 0xFF.

Use the **undo ft1 idlecode** command to restore the default, that is, 0x7E.

The line idle code is sent in the timeslots that are not bundled into the logical channels on the interface.

Example # Set the line idle code to 0x7E on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 idlecode 7e
```

ft1 itf

Syntax **ft1 itf** { **number** *number* | **type** { **7e** | **ff** } }

undo ft1 itf { **type** | **number** }

View T1-F interface view

Parameter **number** *number*: Sets the number of interframe filling tags (a interframe filling tag is one byte in length). The *number* argument ranges from 0 to 14.

type { **7e** | **ff** }: Sets the interframe filling tag to 0x7E by specifying the **7e** keyword or to 0xFF by specifying the **ff** keyword. On a T1-F interface, the default interframe filling tag is 0x7E.

Description Use the **ft1 itf** command to set the type and the number of interframe filling tags on the T1-F interface. Two types of interframe filling tag are available: 0x7E and 0xFF.

Use the **undo ft1 itf** command to restore the default.

By default, the interframe filling tag is 0x7E, and the number of interframe filling tags is four.

Interframe filling tags are sent when no service data is sent on the timeslots bundled into logical channels on a T1-F interface.

Do not use the **ft1 itf type ff** command if both the **ft1 code ami** command and the **ft1 data-coding inverted** command are configured so that the T1-F interface can function normally.

Example # Set the interframe filling tag to 0xFF on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 itf type ff
```

Set the number of interframe filling tags to five on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 itf number 5
```

ft1 loopback

Syntax **ft1 loopback** { **local** | **payload** | **remote** }

undo ft1 loopback

View T1-F interface view

Parameter **local**: Sets the interface in internal loopback mode.

payload: Sets the interface in external payload loopback mode.

remote: Sets the interface in external loopback mode.

Description Use the **ft1 loopback** command to set the T1-F interface in a loopback mode.

Use the **undo ft1 loopback** command to restore the default.

By default, loopback is disabled.

Loopback is intended for checking the condition of interfaces or cables. Disable it otherwise.

The three loopback modes cannot be used at the same time on a T1-F interface.

Example # Set T1-F interface Serial 2/0 in local loopback mode.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0]ft1 loopback local
```

ft1 timeslot-list

Syntax **ft1 timeslot-list** *list* [**speed** { **56k** | **64k** }]

undo ft1 timeslot-list

View T1-F interface view

Parameter *list*: Specifies timeslots to be bundled. They are numbered 1 through 31. You may specify a single timeslot by specifying its number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*.

speed { **56k** | **64k** }: Time slot bundling speed in kbps. If **56k** applies, timeslots are bundled into an N × 56 kbps bundle. If **64k** (the default) applies, timeslots are bundled into an N × 64 kbps bundle.

Description Use the **ft1 timeslot-list** command to bundle timeslots on a T1-F interface.

Use the **undo ft1 timeslot-list** command to restore the default.

By default, all the timeslots on the T1-F interface are bundled to form a 1536 kbps interface.

Timeslot bundling results in interface rate change. For example, after you bundle timeslots 1 through 10 on the interface, the interface rate becomes 10 × 64 kbps or 10 × 56 kbps.

Only one channel set can be created on a T1-F interface, and this channel set is associated with the current synchronous serial interface. On a CT1/PRI interface, however, you may create multiple channel sets; for each of them, the system automatically creates a synchronous serial interface.

Example # Bundle timeslots 1, 2, 5, 10 through 15, and 18 on T1-F interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 timeslot-list 1,2,5,10-15,18
```

ft1 alarm-threshold

Syntax **ft1 alarm-threshold** { **ais** { **level-1** | **level-2** } | **lfa** { **level-1** | **level-2** | **level-3** | **level-4** } | **los** { **pulse-detection** | **pulse-recovery** } *value* }

undo ft1 alarm-threshold

View T1-F interface view

Parameter **ais**: Sets the alarm threshold of alarm indication signal (AIS), which can be **level-1** and **level-2**.

- The **level-1** keyword specifies to generate an AIS alarm when the number of 0s in the bit stream of an SF or ESF frame is less than or equal to 2.
- The **level-2** keyword specifies to generate an AIS alarm when the number of 0s is less than or equal to 3 in the bit stream of an SF frame or less than or equal to 5 in the bit stream of an ESP frame.

By default, level-1 AIS alarm threshold applies.

lfa: Sets the loss of frame align (LFA) alarm threshold, which can be **level-1**, **level-2**, **level-3**, and **level-4**.

- The **level-1** keyword specifies to generate an LFA alarm when two of four frame alignment bits are lost.
- The **level-2** keyword specifies to generate an LFA alarm when two of five frame alignment bits are lost.
- The **level-3** keyword specifies to generate an LFA alarm when two of six frame alignment bits are lost.
- The **level-4** keyword applies only to ESF frames. It specifies to generate an LFA alarm when errors are detected in four consecutive ESF frames.

By default, level-1 LFA alarm threshold applies.

los: Sets a loss of signal (LOS) alarm threshold, which can be **pulse-detection** (for the pulse detection duration threshold with LOS) and **pulse-recovery** (for the pulse threshold with LOS).

The threshold of pulse-detection, in units of pulse intervals, ranges from 16 to 4,096 and defaults to 176.

The threshold of pulse-recovery, ranges from 1 to 256 and defaults to 22.

If the number of the pulses detected during the total length of the specified pulse detection intervals is smaller than the pulse-recovery threshold, a LOS alarm occurs. For example, if the two thresholds take their defaults, a LOS alarm is created if the number of pulses detected within 176 pulse intervals is less than 22.

Description Use the **ft1 alarm-threshold** command to set LOS, AIS, or LFA alarm thresholds on the T1-F interface.

Use the **undo ft1 alarm-threshold** command to restore the defaults.

Example # Set the number of detection intervals to 300 for the pulse detection duration threshold.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 alarm-threshold los pulse-detection 300
```

ft1 sendloopcode

Syntax **ft1 sendloopcode** { **fdl-ansi-llb-down | fdl-ansi-llb-up | fdl-ansi-plb-down | fdl-ansi-plb-up | fdl-att-plb-down | fdl-att-plb-up | inband-llb-down | inband-llb-up** }

View T1-F interface view

Parameter **fdl-ansi-llb-down**: Sends ANSI-compliant LLB deactivation request code in the FDL to removes loopback.

fdl-ansi-llb-up: Sends ANSI-compliant line loopback (LLB) activation request code in the FDL to start remote loopback.

fdl-ansi-plb-down: Sends ANSI-compliant PLB deactivation request code in the FDL to remove loopback.

fdl-ansi-plb-up: Sends ANSI-compliant payload loopback (PLB) activation request code in the FDL to start remote loopback.

fdl-att-plb-down: Sends AT&T-complaint PLB deactivation request code in the FDL to remove loopback.

fdl-att-plb-up: Sends AT&T-complaint PLB activation request code in the FDL to start remote loopback.

inband-llb-down: Sends in-band LLB deactivation request code compliant with the ANSI or AT&T implementation to remove loopback.

inband-llb-up: Sends in-band line loopback (LLB) activation request code compliant with the ANSI or AT&T implementation to start remote loopback.

Description Use the **ft1 sendloopcode** command to send remote loopback control code.

By default, no remote loopback control code is sent.

You may configure loopback on the far-end T1-F interface by sending loopback request code.

In LLB mode, all 193 bits (one synchronization bit and 192 effective bandwidth bits) in a T1 PCM frame are looped back. In PLB mode, however, only 192 effective bandwidth bits are looped back.

The format of loopback code can be compliant with ANSI T1.403 or AT&T TR 54016.

In SF framing, LLB code is sent using the effective bandwidth (slots 1 through 24). In ESF framing, both LLB code and PLB code are sent/received in the FDL in ESF frames.

You can use this command only when the far-end CT1/PRI interface can automatically detect loopback request code from the network.

Example # Send in-band LLB activation request code.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ft1 sendloopcode inband-llb-up
```

16 FUNDAMENTAL CE3 INTERFACE CONFIGURATION COMMANDS

bert (CE3 Interface)

Syntax **bert pattern** { **2^7** | **2^11** | **2^15** | **qrss** } **time** *number* [**unframed**]

undo bert

View CE3 interface view

Parameter **pattern**: Specifies BERT test mode, which can be 2^7, 2^11, 2^15, and QRSS.

2^7: Specifies the code stream transmitted is the 7th power of 2 bits in length.

2^11: Specifies the code stream transmitted is the 11th power of 2 bits in length.

2^15: Specifies the code stream transmitted is the 15th power of 2 bits in length.

qrss: Specifies the code stream transmitted is the 20th power of 2 bits in length and the number of successive 0s in the code stream is no more than 14.

time *number*: Sets the duration (in minutes) of a BERT teat. The *number* argument is in the range 1 to 1,440.

unframed: Sets the overhead bits of the padding frames for BERT test.

Description Use the **bert** command to enable BERT test.

Use the **undo bert** command to disable BERT test.

Multiple BERT test modes exist, as defined in ITU O.151, ITU O.153, and ANSI T1.403-1999. Currently, 2^7, 2^11, 2^15, and QRSS are available on a CE3 interface.

To perform a BERT test, the local end transmits test data stream, which is returned after reaching specific nodes. The local end then checks for the bit error rate by comparing the returned data stream with the original, through which the state of the link can be determined. BERT test requires that data stream can be looped back on specific nodes. You can achieve this by enabling remote loop back on the peer.

You can use the **bert** command to set the test mode and the test duration. During the process of a BERT test, you can check the state and the result of the test. For more information, refer to “display controller e1” on page 205.

Example # Perform BERT test in QRSS mode on CE3 2/0 interface, setting the duration to ten minutes.

```
<Sysname> system-view
[Sysname] interface E3 2/0
[Sysname-E3 2/0] bert pattern qrss time 10
```

clock (CE3 interface view)

Syntax **clock** { **master** | **slave** }

undo clock

View CE3 interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **clock** command to configure clock source for the CE3 interface.

Use the **undo clock** command to restore the default, that is, line clock.

The clock source is selected depending on the connected remote device. If connected to a transmission device, the local end uses the line clock. If connected to a CE3 interface on another router, the local end can use whichever clock so long as it is different from the one adopted at the remote end.

Example # Use the internal clock as the clock source on CE3 interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] clock master
```

controller e3

Syntax **controller e3** *interface-number*

View System view

Parameter *interface-number*: CE3 interface number.

Description Use the **controller e3** command to enter CE3 interface view.

Related command: **display controller e3**.

Example # Enter the view of interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0]
```

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit CRC.

32: Adopts 32-bit CRC.

none: Adopts no CRC.

Description Use the **crc** command to configure CRC mode for a synchronous serial interface formed by CE3 interfaces.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

Related command: **e1 channel-set**, **e1 unframed**, **using (CT3 interface view)**.

Example # Apply 32-bit CRC to a serial interface formed on interface E3 2/0 in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] using e3
[Sysname-E3 2/0] quit
[Sysname] interface serial 2/0/0:0
[Sysname-Serial2/0/0:0] crc 32
```

Apply 16-bit CRC to a serial interface formed on interface E3 2/0 in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] t1 3 channel-set 5 timeslot-list 1-20
[Sysname-E3 2/0] quit
[Sysname] interface serial 2/0/3:5
[Sysname-Serial2/0/3:5] crc 16
```

display controller e3

Syntax **display controller e3** [*interface-number*]

View Any view

Parameter *interface-number*: CE3 interface number. In conjunction with the **e3** keyword, it specifies a CE3 interface.

Description Use the **display controller e3** command to display state information about one specified or all CE3 interfaces.

In addition to the state information of the CE3 interface, the command displays information about each E1 line on the CE3 interface if the interface is working in CE3 mode.

Example # Display information about interface E3 2/0.

```
<Sysname> display controller e3 2/0
  E3 2/0 is up
  Description : E3 2/0 Interface
  Applique type is CE3 - 75 OHM unbalanced  Frame-format G751, line
code HDB3, clock slave, national-bit 1,loopback not set
  Alarm: none
  ERROR: 0 BPV, 0 EXZ, 0 FrmErr, 0 FEBE
E3-0  CE1 1 is up
  Frame-format NO-CRC4, clock master, loopback not set
E3-0  CE1 2 is up
  Frame-format NO-CRC4, clock slave, loopback local
E3-0  CE1 3 is up
  Frame-format NO-CRC4, clock slave, loopback remote
E3-0  CE1 4 is up
  Frame-format CRC4, clock slave, loopback not set
E3-0  CE1 5 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 6 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 7 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 8 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 9 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 10 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 11 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 12 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 13 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 14 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 15 is up
  Frame-format NO-CRC4, clock slave, loopback not set
E3-0  CE1 16 is up
  Frame-format NO-CRC4, clock slave, loopback not set
```

e1 bert

Syntax **e1** *line-number* **bert pattern** { **2^11** | **2^15** | **2^20** | **2^23** | **qrss** } **time** *number* [**unframed**]

undo e1 *line-number* **bert**

View CE3 interface view

Parameter *line-number*: E1 channel number, in the range 1 to 28.

pattern: Specifies BERT test mode, which can be 2^11, 2^15, 2^20, 2^23, and QRSS.

2^11: Specifies the code stream transmitted is the 11th power of 2 bits in length.

2^15: Specifies the code stream transmitted is the 15th power of 2 bits in length.

2^20: Specifies the code stream transmitted is the 20th power of 2 bits in length.

2^23: Specifies the code stream transmitted is the 23th power of 2 bits in length.

qrss: Specifies the code stream transmitted is the 20th power of 2 bits in length and the number of successive 0s in the code stream is no more than 14.

time *number*: Sets the duration (in minutes) of a BERT teat. The *number* argument is in the range 1 to 1,440.

unframed: Sets the overhead bits of the padding frames for BERT test.

Description Use the **e1 bert** command to enable BERT test for an E1 channel created on a CE3 interface.

Use the **undo e1 bert** command to disable BERT test.

Multiple BERT test modes exist, as defined in ITU O.151, ITU O.153, and ANSI T1.403-1999. Currently, 2^11, 2^15, 2^20, 2^23, and QRSS are available on E1 channels created on CE3 interfaces.

To perform a BERT test, the local end transmits test data stream, which is returned after reaching specific nodes. The local end then checks for the bit error rate by comparing the returned data stream with the original, through which the state of the link can be determined. BERT test requires that data stream can be looped back on specific nodes. You can achieve this by enabling remote loop back on the peer.

You can use the **bert** command to set the test mode and the test duration. During the process of a BERT test, you can check the state and the result of the test. For more information, refer to “display controller e1” on page 205.

Example # Perform BERT test in QRSS mode on E1 channel 1 created on CE3 2/0 interface, setting the duration to ten minutes.

```
<Sysname> system-view
[Sysname] interface e3 2/0
[Sysname-E3 2/0] e1 1 bert pattern qrss time 10
```

e1 channel-set

Syntax **e1** *line-number* **channel-set** *set-number* **timeslot-list** *list*

undo e1 *line-number* **channel-set** *set-number*

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

set-number: Number of the channel set formed by a timeslot bundle on the E1 line. It ranges from 0 to 30.

timeslot-list *list*: Specifies timeslots to be bundled. The *list* argument is timeslot numbers, in the range of 1 to 31. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1***-***number2*, or several discrete timeslots by specifying *number1*, *number2***-***number3*.

Description Use the **e1 channel-set** command to bundle timeslots on an E1 line.

Use the **undo e1 channel-set** command to remove a timeslot bundle.

By default, no timeslots are bundled into channel sets.

A CE3 interface can be channelized into 64 kbps lines and the timeslots on each E1 line can be bundled into up to 31 channels.

When an E1 line operates in framed (CE1) mode, you can bundle timeslots on it into channel sets. For each channel set, the system automatically creates a serial interface numbered **serial** *number***/***line-number***:***set-number*. For example, the serial interface formed by channel set 0 on the first E1 line on E3 1/0 is numbered 1/0/1:0. This interface can operate at N × 64 kbps and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Related command: **e1 unframed**.

Example # Create a 128 kbps serial interface on the first E1 channel on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 channel-set 1 timeslot-list 1,2
```

e1 set clock

Syntax **e1** *line-number* **set clock** { **master** | **slave** }

undo e1 *line-number* **set clock**

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

master: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **e1 set clock** command to configure clock source for an E1 line on the CE3 interface.

Use the **undo e1 clock** command to restore the default, that is, line clock.

When the CE3 interface is working in channelized mode, you can set separate clock for each E1 line on it.

Example # Use the internal clock as the clock source on the first E1 line on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 set clock slave
```

e1 set frame-format

Syntax **e1** *line-number* **set frame-format** { **crc4** | **no-crc4** }

undo e1 *line-number* **set frame-format**

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

crc4: Sets the frame format to CRC4.

no-crc4: Sets the frame format to no-CRC4.

Description Use the **e1 set frame-format** command to set framing format for an E1 line.

Use the **undo e1 set frame-format** command to restore the default, that is, no-CRC4.

Configure this command only when the specified E1 line is working in framed format (which can be set using the **undo e1 unframed** command).

Related command: **e1 unframed**.

Example # Set the framing format to CRC4 for the first E1 line on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 set frame-format crc4
```

e1 set loopback

Syntax **e1** *line-number* **set loopback** { **local** | **payload** | **remote** }

undo e1 *line-number* **set loopback**

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

local: Sets the E1 line in internal loopback mode.

payload: Sets the E1 line in payload loopback mode.

remote: Sets the E1 line in external loopback mode.

Description Use the **e1 set loopback** command to set an E1 line in a loopback mode on the E3 interface.

Use the **undo e1 set loopback** command to restore the default.

By default, loopback is disabled on E1 lines.

If an E1 line encapsulated with PPP is in loopback mode, it is normal that the state of the link layer protocol is reported down.

Example # Set the first E1 line on interface E3 2/0 in internal loopback mode.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 set loopback local
```

e1 shutdown

Syntax **e1** *line-number* **shutdown**

undo e1 *line-number* **shutdown**

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

Description Use the **e1 shutdown** command to shut down an E1 line on the CE3 interface.

Use the **undo e1 shutdown** command to restore the default.

By default, E1 lines are up.

This command affects not only the specified E1 line but also the serial interfaces formed by E1 line bundling. Performing the **e1 shutdown** command on the specified E1 line shuts down all these serial interfaces. Data transmission and receiving stop as a result. Likewise, performing the **undo e1 shutdown** command restarts all these serial interfaces.

Example # Shut down the first E1 line on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 shutdown
```

e1 unframed

Syntax **e1** *line-number* **unframed**

undo e1 *line-number* **unframed**

View CE3 interface view

Parameter *line-number*: E1 line number in the range 1 to 16.

Description Use the **e1 unframed** command to set an E1 line on the CE3 interface to work in unframed mode (E1 mode).

Use the **undo e1 unframed** command to restore the default.

By default, an E1 line operates in framed mode (CE1 mode).

An E1 line in unframed mode does not contain the frame control information; it cannot be divided into timeslots. The system automatically creates a serial interface numbered **serial** *number***/***line-number***:0** for it. This interface operates at 2048 kbps and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Related command: **e1 channel-set**.

Example # Set the first E1 line on interface E3 2/0 to operate in unframed mode.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] e1 1 unframed
```

fe3

Syntax **fe3** { **dsu-mode** { **0** | **1** } | **subrate** *number* }

undo fe3 { **dsu-mode** | **subrate** }

View CE3 interface (in FE3 mode) view

Parameters **dsu-mode**: Specifies the FE3 (Fractional E3) DSU mode for a CE3 interface operating in FE3 mode. This keyword can be followed by **0** or **1** keyword, as described below:.

0: Specifies the Digital Link mode, where the subrate is a multiple of 358 kbps and ranges from 358 to 34010 kbps (that is, up to 95 rate levels are available).

1: Specifies the Kentrox mode, where the subrate is a multiple of 500 kbps and ranges from 500 to 24500 kbps. In this mode, the subrate can also be 34010 kbps, making a total of 50 rate levels.

subrate *number*: Specifies the subrate for the CE3 interface. The *number* argument ranges from 1 to 34010 (in kbps).

Description Use the **fe3** command to configure a CE3 interface to operate in the FE3 mode and set the DSU mode or the subrate.

Use the **undo fe3** command to restore the default.

By default, DSU mode 1 (the Kentrox mode) is adopted, and the subrate is 34010 kbps.

FE3 mode is a non-standard E3 application mode. In this mode, the subrate level setting varies with vendors. You can use the **fe3** command to make the device to be compatible with devices of other vendors operating in specific FE3 DSU modes.

Note that:

- These two commands are only applicable to CE3 boards that support FE3.
- These two commands are only available in E3 mode.
- As for the **fe3 subrate** command, the actual subrate usually is not exactly the one set by the command. That is, after you set the subrate by using the **fe3 subrate** command, the CE3 interface searches the subrate levels corresponding to the DSU mode it is operating in and selects the one that is closest to that set by the command as its subrate. The device then adjusts the hardware to allow for the subrate.
- You can use the **display interface serial interface-number:0** command to check the DSU mode setting, the subrate, the actual rate, and the baudrate of a CE3 interface. Note that the actual rate does not count in the overhead bits, and the baudrate is the actual E3 line rate (that is, 34368 kbps), with the overhead bits counted in.

Examples # Configure E3 2/0 interface to operate in the FE3 mode, setting the DSU mode to 1 and the subrate to 3000 kbps.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] using e3
[Sysname-E3 2/0] fe3 dsu-mode 1
[Sysname-E3 2/0] fe3 subrate 3000
```

loopback (CE3 interface view)

Syntax **loopback { local | payload | remote }**

undo loopback

View CE3 interface view

Parameter **local**: Enables internal loopback on the CE3 interface.

payload: Enables external payload loopback on the CE3 interface.

remote: Enables external loopback on the CE3 interface.

Description Use the **loopback** command to configure the loopback mode of the CE3 interface.

Use the **undo loopback** command to restore the default.

By default, loopback is disabled on the CE3 interface.

Loopback is intended for test use. Disable it otherwise.

If a CE3 interface encapsulated with PPP is placed in a loopback, it is normal that the state of the link layer protocol is reported down.

Example # Enable internal loopback on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] loopback local
```

national-bit

Syntax **national-bit { 0 | 1 }**

undo national-bit

View CE3 interface view

Parameter **0**: Sets the national bit of the CE3 interface to 0.

1: Sets the national bit of the CE3 interface to 1.

Description Use the **national-bit** command to configure the national bit on the CE3 interface.

Use the **undo national-bit** command to restore the default, that is, 1.

You need to set the national bit to 0 on an E3 interface only in some special circumstances.

Related command: **controller e3**.

Example # Set the national bit to 0 on interface E3 2/0.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] national-bit 0
```

using (CE3 interface view)

Syntax **using** { **ce3** | **e3** }

undo using

View CE3 interface view

Parameter **ce3**: Sets the CE3 interface to work in channelized mode.

e3: Sets the CE3 interface to work in unchannelized mode.

Description Use the **using** command to configure the operating mode of the CE3 interface.

Use the **undo using** command to restore the default, that is, channelized mode.

Only when the CE3 interface is working in channelized mode can you configure E1 lines.

When the CE3 interface is working in unchannelized mode, the system automatically creates a serial interface numbered **serial** *number***/0:0** for it. This interface operates at 34.368 Mbps and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Related command: **controller e3**.

Example # Configure interface E3 2/0 to operate in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller e3 2/0
[Sysname-E3 2/0] using e3
```

17 FUNDAMENTAL CT3 INTERFACE CONFIGURATION COMMANDS

alarm (CT3 interface view)

Syntax **alarm** { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }

undo alarm { **detect** | **generate** { **ais** | **febe** | **idle** | **rai** } }

View CT3 interface view

Parameter **detect**: Enables/disables periodical alarm signal detection. By default, periodical alarm detection is enabled.

generate: Sends alarm signals, which can be AIS, RAI, idle, or FEBE for line state test. By default, alarm signal sending is disabled.

ais: Alarm indication signal.

febe: Far end block error signal.

idle: Idle signal.

rai: Remote alarm indication signal.

Description Use the **alarm** command to enable the CT3 interface to detect/send alarm signals.

Use the **undo alarm** command to remove the alarm signal detection/sending setting.

At the startup of your device, periodical alarm signal detection is enabled on the CT3 interface. When detecting LOS, LOF, or AIS signals, the interface sends RAI signals to its peer. Alarm state report for the interface is real time; you may view that by performing the **display controller t3** command.

The supported alarm signals, LOS, LOF, AIS, RAI, FEBE, and idle, are ANSI T1.107-1995 compliant.

You can only configure the CT3 interface to send a type of alarm signal. To have the interface send another type of signal, use the **undo alarm** command to remove the previous setting first. In addition, when the RAI signal generated upon detection of the LOS, LOF, or AIS signal is present, the CT3 interface cannot send another type of signal. To do that, use the **undo alarm detect** command to disable the CT3 interface to send the RAI signal generated after detecting an alarm first.

Example # Enable periodical alarm signal detection on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] alarm detect
```

Enable CT3 interface T3 2/0 to send AIS alarm signals.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] alarm generate ais
```

bert (CT3 interface view)

Syntax **bert pattern** { **2^7** | **2^11** | **2^15** | **qrss** } **time** *number* [**unframed**]

undo bert

View CT3 interface view

Parameter **pattern**: Sets a bit error rate test (BERT) pattern, which could be 2^7, 2^11, 2^15, or QRSS.

2^7: Two to the seventh power, length of the transmitted BERT pattern in bits.

2^11: Two to the eleventh power, length of the transmitted BERT pattern in bits.

2^15: Two to the fifteenth power, length of the transmitted BERT pattern in bits.

qrss: Two to the twentieth power, length of the transmitted BERT pattern in bits. In this pattern, the presence of 14 consecutive zeros is not allowed.

time *number*: Sets the duration of a BERT test, in the range 1 to 1440 minutes.

unframed: Sets the test pattern to cover the overhead bits of the frame.

Description Use the **bert** command to start a BERT test on the CT3 interface.

Use the **undo bert** command to stop the BERT test running on the CT3 interface.

ITU O.151, ITU O.153, and ANSI T1.403-1999 define many BERT patterns, among which, the CT3 interface supports only 2^7, 2^11, 2^15, and QRSS at present.

When running a BERT test, the local end sends out a pattern, which is to be looped over somewhere on the line and back to the local end. The local end then checks the received pattern for bit error rate, and by so doing helps you identify whether the condition of the line is good. To this end, you must configure loopback to allow the transmitted pattern to loop back from somewhere on the line, for example, from the far-end interface by placing the interface in far-end loopback.

You may view the state and result of the BERT test with the **display controller t3** command.

Example # Run a 10-minute QRSS BERT test on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] bert pattern qrss time 10
```

cable (CT3 interface view)

Syntax **cable** *feet*

undo cable

View CT3 interface view

Parameter *feet*: Cable length in the range 0 to 450 feet (0 to 137.2 meters).

Description Use the **cable** command to configure the cable length on the CT3 interface.

Use the **undo cable** command to restore the default, that is, 49 feet (14.9 meters).

The cable length in this command refers to the distance between the router and the cable distribution rack.

Example # Set the cable length to 50 feet (15.2 meters) on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] cable 50
```

clock (CT3 interface view)

Syntax **clock** { **master** | **slave** }

undo clock

View CT3 interface view

Parameter **master**: Adopts the internal clock as the clock source.

slave: Adopts the line clock as the clock source.

Description Use the **clock** command to configure clock source for the CT3 interface.

Use the **undo clock** command to restore the default, that is, line clock.

The clock source is selected depending on the connected remote device. If connected to a transmission device, the local end uses the line clock. If connected to a CT3 interface on another router, the local end can use whichever clock so long as it is different from the one adopted at the remote end.

Example # Use the internal clock as the clock source on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] clock master
```

controller t3

Syntax **controller t3** *interface-number*

View System view

Parameter *interface-number*: CT3 interface number.

Description Use the **controller t3** command to enter CT3 interface view.

Related command: **display controller t3**.

Example # Enter the view of interface T3 2/0.

```
<Sysname> system-view
[Sysname] controller t3 2/0
[Sysname-T3 2/0]
```

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronous serial interface view

Parameter **16**: Adopts 16-bit CRC.

32: Adopts 32-bit CRC.

none: Adopts no CRC.

Description Use the **crc** command to configure CRC mode for the serial interface formed on CT3 interfaces.

Use the **undo crc** command to restore the default, that is, 16-bit CRC.

These two commands apply to serial interfaces formed on T3 channels, T1 channels, and the interfaces formed by binding slots of T1 channels.

Related command: **t1 channel-set**, **t1 unframed**, **using (CT3 interface view)**.

Example # Apply 32-bit CRC to a serial interface formed on interface T3 2/0 in unchannelized mode.

```
<Sysname> system-view
[Sysname] controller t3 2/0
[Sysname-T3 2/0] using t3
[Sysname-T3 2/0] quit
[Sysname] interface serial 2/0/0:0
[Sysname-Serial2/0/0:0] crc 32
```

Apply 16-bit CRC to a serial interface formed on interface CT3 2/0 in channelized mode.

```
<Sysname> system-view
[Sysname] controller t3 2/0
[Sysname-T3 2/0] t1 2 channel-set 4 timeslot-list 5-11
[Sysname-T3 2/0] quit
[Sysname] interface serial 2/0/2:4
[Sysname-Serial2/0/2:4] crc 16
```

display controller t3

Syntax **display controller t3** [*interface-number*]

View Any view

Parameter *interface-number*: CT3 interface number. In conjunction with the **t3** keyword, it specifies a CT3 interface.

Description Use the **display controller t3** command to display state information about one specified or all CT3 interfaces.

In addition to the state information about the CT3 interface, the command displays information about each T1 line on the CT3 interface if the interface is working in CT3 mode.

Example # Display information about interface T3 2/0.

```
<Sysname> display controller t3 2/0
T3 2/0 current state :UP
Description : T3 2/0 Interface
sic Configuration:
  Work mode is CT3, cable length is 49 feet.
  Frame-format is C-BIT Parity, line code is B3ZS.
  Source clock is slave, loopback is not set.
Alarm state:
  Receiver alarm state is none.
MDL state:
  No message is sent now.
  Message data elements:
    EIC: line, LIC: line, FIC: line, UNIT: line
    FI: line, PORT_NO: line, GEN_NO: line
  Periodical detection is disabled.
FEAC state:
```

```
  No code is sent now.
  Periodical detection is enabled, no code received now.
BERT state:(stopped, not completed)
  Test pattern: 2^7, Status: Not Sync, Sync Detected: 0
    Time: 0 minute(s), Time past: 0 minute(s)
    Bit errors (since test started): 0 bits
    Bits received (since test started): 0 Mbits
    Bit errors (since latest sync): 0 bits
    Bits received (since latest sync): 0 Mbits
Historical Statistics:
Last clearing of counters: 14:39:02 UTC Sat 06/25/2005
  Data in current interval (22 seconds elapsed):
    0 Line Code Violations, 0 Far End Block Error
    0 C-Bit Coding Violation, 0 P-bit Coding Violation
    0 Framing Bit Err, 0 Severely Err Framing Secs
    0 C-bit Err Secs, 0 C-bit Severely Err Secs
    0 P-bit Err Secs, 0 P-bit Severely Err Secs
    0 Unavailable Secs, 0 Line Err Secs

T3 2/0  CT1 1 is up
  Frame-format ESF, clock slave, loopback not set
  FDL Performance Report is disabled
  Transmitter is sending none
  Receiver alarm state is none
  Line loop back deactivate code using inband signal last sent
  BERT state:(stopped, not completed)
    Test pattern: 2^11, Status: Not Sync, Sync Detected: 0
    Time: 0 minute(s), Time past: 0 minute(s)
    Bit errors (since test started): 0 bits
    Bits received (since test started): 0 Kbits
    Bit errors (since latest sync): 0 bits
    Bits received (since latest sync): 0 Kbits
```

Table 21 Description on the fields of the display controller t3 command

Field	Description
T3 2/0 current state	Physical state of the interface: up or down
Description : T3 2/0 Interface	Description about the interface
Basic Configuration	Basic configurations of the interface
Work mode	Operating mode of the interface, CT3 or T3.
cable length	Cable length supported by the interface
Frame-format	Frame format: C-bit parity or M23
line code	In this output sample, line code is B3ZS.
Source clock	Clock source used by the interface: master for the internal clock or slave for the line clock
loopback	Loopback setting on the interface: local, remote, payload, or not set
Alarm State	Alarm state
Receiver alarm state	Type of the received alarm: none, LOS, LOF, RAI, or AIS. If a LOS, LOF, AIS was received, RAI would be sent and the screen displayed "Transmitter is sending RAI" instead.
MDL state	MDL state

Table 21 Description on the fields of the display controller t3 command

Field	Description
No message is sent now.	No MDL message is being sent. If an MDL message, path or idle-signal for example, was being sent, the screen would display "Message sent now: path. idle signal."
Message data elements	MDL data elements
EIC: line, LIC: line, FIC: line, UNIT: line	EIC, LIC, FIC, and UNIT are four elements present in all types of MDL messages. Their values are user configurable and default to line.
FI: line, PORT_NO: line, GEN_NO: line	FI is found in MDL path messages, PORT_NO in MDL idle signal messages, and GEN_NO in MDL test signal messages. Their values are user configurable and default to line.
Periodical detection	State of periodical detection of MDL, disabled by default at the startup of the router.
	When the function is enabled, the screen displays:
	Periodical detection is enabled.
	No message was received.
	When MDL messages are detected, the screen displays:
	Message received now: path.idle signal.
	EIC: line, LIC: line, FIC: line, UNIT: line
	path/FI: line
	idle Signal/PORT_NO: line
FEAC state	FEAC state
No code is sent now. DS3 Line Loop Back Deactivate was last sent.	No FEAC signal is sent. The FEAC signal sent last time is DS3 Line Loop Back Deactivate.
Periodical detection is enabled, no code received now.	Periodical detection of FEAC is enabled. This is the default applied at the startup of the router.
	No FEAC signal is received now.
DS3 Line Loop Back Deactivate last received.	The FEAC signal received last time is DS3 Line Loop Back Deactivate.
BERT state:(stopped, not completed)	BERT state: completed, stopped (not completed), or running.
Test pattern: 2^7, Status: Not Sync, Sync Detected: 0	Test pattern in use (such as 2^7, 2^11, 2^15, and QRSS), 2^7 in this sample output; synchronization state, and the number of detected synchronizations
Time: 0 minute(s), Time past: 0 minute(s)	The duration of the BERT test and the time that has elapsed
Bit errors (since test started): 0 bits	Number of bit errors received since the start of the BERT test
Bits received (since test started)	Number of bits received since the start of the BERT test
Bit errors (since latest sync)	Number of bit errors received since last synchronization
Bits received (since latest sync)	Number of bits received since last synchronization
Historical Statistics	Historical statistics
Last clearing of counters	Time when last counter clearing is performed, for example, 14:39:02 UTC Sat 06/25/2005. If no clearing is performed, "Never" is displayed.

Table 21 Description on the fields of the display controller t3 command

Field	Description
Data in current interval:	Statistics spanning the current 15-minute interval, coving the counts of these items:
Line Code Violations	Line code violations: BPV, or EXZ
Far End Block Error	Far-end block error
C-Bit Coding Violation	C-bit coding violation
P-bit Coding Violation	P-bit coding violation
Framing Bit Err	Framing bit error
Severely Err Framing Secs	C-bit erroneous second
C-bit Err Secs	C-bit severely erroneous second, that is, the second during which 44 C-bit errors occur
C-bit Severely Err Secs	P-bit erroneous second
P-bit Err Secs	P-bit severely erroneous second, that is, the second during which 44 P-bit errors occur
P-bit Severely Err Secs	Service unavailable second
Unavailable Secs	Line erroneous second, during which LOS, BPV, EXZ, C-bit, P-bit, and other errors occur
Line Err Secs	Data in interval 1
	Total data spanning the last 17 intervals
Data in Interval 1	State of T1 line on the CT3 interface: up or down. In this output sample, T1 line 1 is up.
Total Data (last 17 15 minute intervals)	Information about the T1 line:
T3 2/0 CT1 1 is up	Framing format-ESF or SF
Frame-format ESF, clock slave, loopback not set	Clock source-slave for the line clock and master for the internal clock
	Loopback-Local, remote, payload, or not set
	Transmission of PPR in the FDL is disabled. You may enable that with the **t1 set fdl ansi** command.
FDL Performance Report is disabled	The transmitter of the T1 line is sending RAI signals. When the T1 line receives LOS, LOF, or AIS signals, it sends RAI signals.
Transmitter is sending RAI	The type of alarm signal that the T1 line can receive: LOS, LOF, AIS, or RAI
Receiver alarm state is LOF	The loopback code sent last time is in-band LLB activation request code.
Line loop back activate code using inband signal last sent	BERT test state: running, complete, or stopped (not completed)
BERT state	Test pattern in use, 2^11 in this sample output; synchronization state, and the number of detected synchronizations
Test pattern	
Status	
Sync Detected	
Time	The duration of the BERT test and the time that has elapsed
Time past	
Bit errors (since test started)	Number of bit errors received since the start of the BERT test
Bits received (since test started)	Number of bits received since the start of the BERT test
Bit errors (since latest sync)	Number of bit errors received since the last synchronization

Table 21 Description on the fields of the display controller t3 command

Field	Description
Bits received (since latest sync)	Number of bits received since the last synchronization

feac (CT3 interface view)

Syntax **feac** { **detect** | **generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** | **loopback** { **ds3-line** | **ds3-payload** } } }

undo feac { **detect** | **generate** { **ds3-los** | **ds3-ais** | **ds3-oof** | **ds3-idle** | **ds3-eqptfail** | **loopback** { **ds3-line** | **ds3-payload** } } }

View CT3 interface view

Parameter **detect**: Enables periodical far end and control signal (FEAC) channel signal detection. By default, periodical FEAC channel signal detection is enabled.

generate: Sends FEAC signals. Specify **ds3-los** for DS3 LOS, **ds3-ais** for DS3 AIS, **ds3-oof** for DS3 out of frame (OOF), **ds3-idle** for DS3 idle, and **ds3-eqptfail** for DS3 equipment failure. By default, FEAC signal sending is disabled.

loopback: Sends loopback code for activating far-end line loopback with the **ds3-line** keyword or payload loopback with the **ds3-payload** keyword. By default, loopback code sending is disabled.

Description Use the **feac** command to enable FEAC channel signal detection and sending on the CT3 interface.

Use the **undo feac** command to remove the current FEAC settings.

FEAC is a channel formed by using the third C-bit in the first subframe in C-bit framing. It is used to transmit alarm state signals for line test purpose or to transmit loopback control code for activating or deactivating far-end loopback during a loopback test.

According to ANSI T1.107a, the frame format used by FEAC channels is bit oriented protocol (BOP).

At the startup of your router, FEAC channel signal detection is enabled on the CT3 interface with FEAC signal sending disabled.

After far-end loopback is activated with the **feac generate loopback** { **ds3-line | ds3-payload** } command, you may remove it with the **undo** form of the command.

Disable FEAC detection before you configure far-end loopback to prevent loopback deadlock, which may happen when the local end enables loopback after detecting the loopback code sent back by the far end.

You may view the transmitting/receiving state of the FEAC channel with the **display controller t3** command.

Example # Enable FEAC channel signal detection on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] feac detect
```

Sends DS3 LOS signal on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] feac generate ds3-los
```

On CT3 interface T3 2/0, send loopback code to the far end to place the far end in a line loopback.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] feac generate loopback ds3-line
```

frame-format (CT3 interface view)

Syntax **frame-format** { **c-bit** | **m23** }

undo frame-format

View CT3 interface view

Parameter **c-bit**: Sets the framing format to C-bit.

m23: Sets the framing format to m23.

Description Use the **frame-format** command to configure the framing format used by the CT3 interface.

Use the **undo frame-format** command to restore the default, that is, C-bit framing format.

Example # Set the framing format of interface T3 2/0 to m23.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] frame-format m23
```

ft3

Syntax **ft3** { **dsu-mode** { **0** | **1** | **2** | **3** | **4** } | **subrate** *number* }

undo ft3 { **dsu-mode** | **subrate** }

View CT3 interface (in FT3 mode) view

Parameters **dsu-mode**: Specifies the FT3 (Fractional T3) DSU mode for a CT3 interface operating in FT3 mode. This keyword can be followed by **0**, **1**, **2**, **3**, and **4**, as described below.

0: Specifies the Digital Link mode, where the subrate is a multiple of 300746 bps and ranges from 300 to 44210 kbps (that is, up to 147 rate levels are available).

1: Specifies the Kentrox mode, where the subrate is a multiple of 1500 kbps and ranges from 1500 to 35000 kbps. In this mode, the subrate can also be 44210 kbps, making a total of 57 subrate levels.

2: Specifies the Larscom mode, where the subrate is a multiple of 3157835 bps and ranges from 3100 to 44210 kbps (that is, up to 14 subrate levels are available).

3: Specifies the Adtran mode, where the subrate is a multiple of 75187 bps and ranges from 75 to 44210 kbps (that is, up to 588 subrate levels are available).

4: Specifies the Verilink mode, where the subrate is a multiple of 1578918 bps and ranges from 1500 to 44210 kbps (that is, up to 20 subrate levels are available).

subrate *number*: Specifies the subrate for the CT3 interface. The *number* argument ranges from 1 to 44210 (in kbps).

Description Use the **ft3** command to configure a CT3 interface to operate in the FT3 mode and set the DSU mode or the subrate.

Use the **undo ft3** command to restore the default.

By default, DSU mode 0 (the Digital Link mode) is adopted, and the subrate is 44210 kbps.

FT3 (Fractional T3 or Subrate T3) mode is a non-standard E3 application mode. In this mode, the subrate level setting varies with vendors. You can use the **ft3** command to make the device to be compatible with devices of other vendors operating in specific FT3 DSU modes.

Note that:

- These two commands are only applicable to CT3 boards that support FT3.
- These two commands are only available in T3 mode.
- As for the **ft3 subrate** command, the actual subrate usually is not exactly the one set by the command. That is, after you set the subrate by using the **ft3 subrate** command, the CT3 interface searches the subrate levels corresponding to the DSU mode it is operating in and selects the one that is closest to that set by the command as its subrate. The device then adjusts the hardware to allow for the subrate.
- You can use the **display interface serial interface-number:0** command to check the DSU mode setting, the subrate, the actual rate, and the baudrate of a CT3 interface. Note that the actual rate does not count in the overhead bits, and the baudrate is the actual T3 line rate (that is, 44736 kbps), with the overhead bits counted in.

Examples # Configure T3 2/0 interface to operate in the FT3 mode, setting the DSU mode to 1 and the subrate to 3000 kbps.

```
<Sysname> system-view
[Sysname] controller t3 2/0
[Sysname-T3 2/0] using t3
[Sysname-T3 2/0] ft3 dsu-mode 1
[Sysname-T3 2/0] ft3 subrate 3000
```

loopback (CT3 interface view)

Syntax **loopback** { **local** | **payload** | **remote** }

undo loopback

View CT3 interface view

Parameter **local**: Enables internal loopback on the CT3 interface.

payload: Enables external payload loopback on the CT3 interface.

remote: Enables external loopback on the CT3 interface.

Description Use the **loopback** command to configure the loopback mode for a CT3 interface.

Use the **undo loopback** command to disable loopback.

By default, loopback is disabled on CT3 interfaces.

Loopback is intended for test use. Disable it otherwise.

If a CT3 interface encapsulated with PPP is placed in a loopback, it is normal that the state of the link layer protocol is reported down.

Example # Enable internal loopback on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] loopback local
```

mdl (CT3 interface view)

Syntax **mdl** { **detect** | **data** { **eic** *string* | **fic** *string* | | **gen-no** *string* | **lic** *string* | **pfi** *string* | **port-no** *string* | **unit** *string* } | **generate** { **idle-signal** | **path** | **test-signal** } }

undo mdl [**detect** | **data** [**eic** | **fic** | **gen-no** | **lic** | **pfi** | **port-no** | **unit**] | **generate** [**idle-signal** | **path** | **test-signal**]]

View CT3 interface view

Parameter **detect**: Enables periodical maintenance data link (MDL) message detection.

data: Sets information included in MDL messages. Among all types of information, EIC, LIC, FIC, and unit are defined for all types of MDL messages; PFI is only for path MDL messages; port number is only for idle signal messages; and generator number is only for test signal messages.

eic *string*: Equipment identification code, a string of 1 to 10 characters. The default EIC is line.

lic *string*: Location identification code, a string of 1 to 11 characters. The default LIC is line.

fic *string*: Frame identification code, a string of 1 to 10 characters. The default FIC is line.

unit *string*: Unit, a string of 1 to 6 characters. The default unit is line.

pfi *string*: Path facility identification, a string in the range 1 to 38 characters. The default PFI is line.

port-no *string*: Port number, a string in the range 1 to 38 characters. The default port number is line.

gen-no *string*: Generator number, a string of 1 to 38 characters. The default generator number is line.

generate: Sends specified information with MDL messages, which can be path, idle signal, and/or test signal regularly.

Description

Use the **mdl** command to configure MDL message detection/sending on the CT3 interface.

Use the **undo mdl** command to remove the MDL settings.

Use the **undo mdl detect** command to disable the CT3 interface to detect MDL messages.

Use the **undo mdl generate** command to disable the CT3 interface to send MDL messages.

Use the **undo mdl data** command to restore the default.

MDL is a channel formed by using the three C-bits in the fifth subframe in C-bit framing. According to ANSI T1.107a, it is used to transmit three types of maintenance messages, path, idle signal, and test signal, and its data frame format is LAPD.

At the startup of your router, MDL message detection and sending are disabled on CT3 interfaces and the default MDL message information applies.

Example

Enable MDL detection on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] mdl detect
```

Set LIC to "hello" for CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] mdl data lic hello
```

Send path messages on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] mdl generate path
```

t1 alarm

Syntax **t1** *line-number* **alarm** { **detect** | **generate** { **ais** | **rai** } }

undo t1 *line-number* **alarm** { **detect** | **generate** { **ais** | **rai** } }

View CT3 interface view

Parameter *line-number*: T1 line number, in the range 1 to 28.

detect: Enables/disables periodical alarm signal detection. By default, periodical alarm detection is enabled.

generate: Sends alarm signals, AIS or RAI, for line state test. By default, alarm signal sending is disabled.

ais: Alarm indication signal.

rai: Remote alarm indication signal.

Description Use the **t1 alarm** command to enable the specified T1 line on the CT3 interface to detect/send alarm signals.

Use the **undo t1 alarm** command to remove the alarm signal detection/sending setting.

At the startup of the router, periodical alarm signal detection is enabled on all T1 lines on the CT3 interface. When a T1 line detects LOS, LOF, or AIS signals, it sends RAI signals to its peer. Alarm state report for the interface is real time; you may view that with the **display controller t3** command.

The supported alarm signals, LOS, LOF, AIS, RAI, FEBE, and idle, are ANSI T1.403 compliant.

You can configure a T1 line to send only a type of alarm signal. To have the channel send another type of signal, use the **undo t1 alarm** command to remove the previous setting first. In addition, when the RAI signal generated upon detection of the LOS, LOF, or AIS signal is present, the T1 line cannot send another type of signal. To do that, use the **undo t1 alarm detect** command to disable the T1 line to send the RAI signal generated after detecting an alarm first.

Example # Enable periodical alarm signal detection on T1 line 1 on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 alarm detect
```

Enable T1 line 1 on CT3 interface T3 2/0 to send AIS alarm signals.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 alarm generate ais
```

t1 bert

Syntax **t1** *line-number* **bert pattern** { **2^11** | **2^15** | **2^20** | **2^23** | **qrss** } **time** *number* [**unframed**]

undo t1 *line-number* **bert**

View CT3 interface view

Parameter *line-number*: T1 line number, in the range 1 to 28.

pattern: Sets a BERT pattern, which could be 2^11, 2^15, 2^20, 2^23, or QRSS.

2^11: Two to the eleventh power, length of the transmitted BERT pattern in bits.

2^15: Two to the fifteenth power, length of the transmitted BERT pattern in bits.

2^20: Two to the twentieth power, length of the transmitted BERT pattern in bits.

2^23: Two to the twenty third power, length of the transmitted BERT pattern in bits.

qrss: Two to the twentieth power, length of the transmitted BERT pattern in bits. In this pattern, the presence of 14 or more consecutive zeros is not allowed.

time *number*: Sets the duration of a BERT test, in the range of 1 to 1440 minutes.

unframed: Sets the test pattern to cover the overhead bits of the frame.

Description Use the **t1 bert** command to start a BERT test on the specified T1 line on the CT3 interface.

Use the **undo t1 bert** command to stop the BERT test running on the specified T1 line on the CT3 interface.

ITU O.151, ITU O.153, and ANSI T1.403-1999 define many BERT patterns, among which, T1 lines on CT3 interfaces support only 2^11, 2^15, 2^20, 2^23, and QRSS at present.

When running a BERT test, the local end sends out a pattern, which is to be looped over somewhere on the line and back to the local end. The local end then

checks the received pattern for the bit error rate, and by so doing helps you determine whether the condition of the line is good. To this end, you must configure loopback to allow the transmitted pattern to loop back from somewhere on the line, for example, from the far-end interface by placing the interface in far-end loopback.

You may view the state and result of the BERT test with the **display controller t3** command.

Example # Run a 10-minute QRSS BERT test on T1 line 1 on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 bert pattern qrss time 10
```

t1 channel-set

Syntax **t1** *line-number* **channel-set** *set-number* **timeslot-list** *list* [**speed** { **56k** | **64k** }]

undo t1 *line-number* **channel-set** *set-number*

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

set-number: Number of a channel set formed from a timeslot bundle on the T1 line. It ranges from 0 to 23.

timeslot-list *list*: Specifies timeslots to be bundled. The *list* argument is timeslot numbers, in the range of 1 to 24. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1***-***number2*, or several discrete timeslots by specifying *number1*, *number2***-***number3*.

speed { **56k** | **64k** }: Speed of the timeslot bundle (the channel set) in kbps. If **56k** is selected, the timeslots is bundled into an N × 56 kbps bundle. If **64k**, the default, is selected, the timeslots is bundled into an N × 64 kbps bundle.

Description Use the **t1 channel-set** command to bundle specified timeslots into a channel set on a T1 line.

Use the **undo t1 channel-set** command to remove the specified channel set.

By default, no channel set is created.

When a T1 line is operating in framed (CT1) mode, you can bundle timeslots on it. For each channel set thus formed, the system automatically creates a serial interface numbered **serial** *number***/***line-number***:***set-number*. This interface operates at N × 64 kbps (or N × 56 kbps) and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Related command: **t1 unframed**.

Example # Create a 128 kbps serial interface through timeslot bundling on the first T1 line on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 channel-set 1 timeslot-list 1,2
```

t1 sendloopcode

Syntax **t1** *line-number* **sendloopcode** { **fdl-ansi-line-up** | **fdl-ansi-payload-up** | **fdl-att-payload-up** | **inband-line-up** }

undo t1 *line-number* **sendloopcode** { **fdl-ansi-line-up** | **fdl-ansi-payload-up** | **fdl-att-payload-up** | **inband-line-up** }

View CT3 interface view

Parameter *line-number*: T1 line number, in the range 1 to 28.

fdl-ansi-line-up: Sends ANSI-compliant LLB activation request code in the FDL to start remote loopback.

fdl-ansi-payload-up: Sends ANSI-compliant PLB activation request code in the FDL to start remote loopback.

fdl-att-payload-up: Sends AT&T-compliant PLB activation request code in the FDL to start remote loopback.

inband-line-up: Sends in-band LLB activation request code compliant with the ANSI and AT&T implementation to start remote loopback.

Description Use the **t1 sendloopcode** command to set the loopback mode of the specified far-end T1 line.

Use the **undo t1 sendloopcode** command to remove the corresponding setting.

Loopback is an effective way of diagnosis. You may place a far-end device into loopback mode either at command line on it or by sending loopback control code to it. The types and formats of loopback control code supported on T1 interfaces are compliant with ANSI T1.403.

Loopback can be divided into line loopback and payload loopback. They differ in the sense that the data stream is looped back at the framer with line loopback but not with payload loopback.

You may transmit loopback control code by using the in-band signal (the 192 effective bandwidth bits or all 193 bits of T1) or the FDL in ESF frames.

Example # Send the in-band signal on T1 line 1 on CT3 interface T3 2/0 to place the far-end T1 line in line loopback mode.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 sendloopcode inband-line-up
```

t1 set clock

Syntax **t1** *line-number* **set clock** { **master** | **slave** }

undo t1 *line-number* **set clock**

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

master: Adopts the internal clock as the clock source on the T1 line.

slave: Adopts the line clock as the clock source on the T1 line.

Description Use the **t1 set clock** command to configure clock source for a T1 line on the CT3 interface.

Use the **undo t1 set clock** command to restore the default, that is, line clock.

When a CT3 interface is working in channelized mode, its T1 lines may use separate clocks.

Example # Use the internal clock as the clock source on the first T1 line on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 set clock slave
```

t1 set frame-format

Syntax **t1** *line-number* **set frame-format** { **esf** | **sf** }

undo t1 *line-number* **set frame-format**

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

esf: Set the T1 line to use the ESF format.

sf: Set the T1 line to use the SF format.

Description Use the **t1 set frame-format** command to configure the framing format of a T1 line.

Use the **undo t1 set frame-format** command to restore the default, that is, ESF.

You can configure this command only when the T1 line is working in framed format (which can be set by using the **undo t1 unframed** command).

Related command: **t1 unframed**.

Example # Set the framing format to SF for the first T1 line on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 set frame-format sf
```

t1 set loopback

Syntax **t1** *line-number* **set loopback** { **local** | **remote** | **payload** }

undo t1 *line-number* **set loopback**

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

local: Sets the T1 line in internal loopback mode.

remote: Sets the T1 line in external loopback mode.

remote: Sets the T1 line in payload loopback mode.

Description Use the **t1 set loopback** command to set the loopback mode of a T1 line on the T3 interface.

Use the **undo t1 set loopback** command to disable the T1 line to loop back.

By default, loopback is disabled on T1 lines.

Loopback is intended for test use. Disable it otherwise.

If a T1 line encapsulated with PPP is placed in loopback mode, it is normal that the state of the link layer protocol is reported down.

Example # Enable internal loopback on the first T1 line on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 set loopback local
```

t1 set fdl

Syntax **t1** *line-number* **set fdl** { **ansi** | **att** | **both** | **none**}

undo t1 *line-number* **set fdl**

View CT3 interface view

Parameter *line-number*: T1 line number, in the range 1 to 28.

fdl: Sets the FDL format of T1.

ansi: Adopts ANSI T1.403 for FDL.

att: Adopts AT&T TR 54016 for FDL.

both: Adopts both ANSI T1.403 and AT&T TR 54016 for FDL.

none: Disables the use of FDL on the T1 line.

Description Use the **t1 set fdl** command to set the behavior of the specified T1 line on the FDL in ESF framing.

Use the **undo t1 set fdl** command to disable FDL of T1.

By default, FDL is disabled.

FDL is an embedded 4 kbps overhead channel within the ESF format for transmitting periodical performance report (PPR) statistics or loopback code.

According to ANSI T1.403, the format of PPR is LAPD, and the format of loopback code is BOP.

The **t1 set fdl** command only starts PPR transmission. It cannot enable loopback code transmission or detection.

These two commands only apply to channelized T1 lines with their T1 frame format being ESF.

Example # Set the FDL to be ANSI T1.403 compliant for T1 line 1 on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 set fdl ansi
```

t1 show

Syntax **t1** *line-number* **show**

View CT3 interface view

Parameter *line-number*: T1 line number, in the range 1 to 28.

show: Displays the physical line state of the specified T1 line.

Description Use the **t1 show** command to have a quick look at the line state of the specified T1 line on the CT3 interface.

Example # Display line state of T1 line 1 on CT3 interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 show
T3 2/0  CT1 1 is up
  Frame-format ESF, clock slave, loopback not set
  FDL Performance Report is disabled
  Transmitter is sending none
  Receiver alarm state is none
  Line loop back deactivate code using inband signal last sent
  BERT state:(stopped, not completed)
    Test pattern: 2^11, Status: Not Sync, Sync Detected: 0
    Time: 0 minute(s), Time past: 0 minute(s)
    Bit errors (since test started): 0 bits
    Bits received (since test started): 0 Kbits
    Bit errors (since latest sync): 0 bits
    Bits received (since latest sync): 0 Kbits
```

Table 22 Description on the fields of the t1 show command

Field	Description
T3 2/0 CT1 1 is up	The state of T1 line 1 on the CT3 interface: up or down
Frame-format ESF	Framing format of T1: ESF or SF
clock slave	Clock source used by the T1 line: slave for the line clock or master for the internal clock
loopback not set	Loopback state or mode: local, remote, payload, or not set.
FDL Performance Report is disabled	Transmission of PPR in the FDL is disabled. You may enable that with the **t1 set fdl ansi** command.
Transmitter is sending RAI	The transmitter of the T1 line is sending RAI signals. When the T1 line receives LOS, LOF, or AIS signals, it sends RAI signals.
Receiver alarm state	The type of alarm signal that the T1 line can receive: LOS, LOF, AIS, or RAI.
Line loop back activate code using inband signal last sent	The loopback code sent last time is in-band LLB activation request code.
BERT state	BERT test state: running, complete, or stopped (not completed)
Test pattern	Test pattern in use, 2^11 in this example; synchronization state, and the number of detected synchronizations
Status	
Sync Detected	
Time	The duration of the BERT test and the time that has elapsed
Time past	
Bit errors (since test started)	Number of bit errors received since the start of the BERT test
Bits received (since test started)	Number of bits received since the start of the BERT test
Bit errors (since latest sync)	Number of bit errors received since the last synchronization
Bits received (since latest sync)	Number of bits received since the last synchronization

t1 shutdown

Syntax **t1** *line-number* **shutdown**

undo t1 *line-number* **shutdown**

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

Description Use the **t1 shutdown** command to shut down a T1 line on the CT3 interface.

Use the **undo t1 shutdown** command to bring up a T1 line.

By default, T1 lines are up.

This command shuts down not only the specified T1 line but also the serial interfaces formed on it. Data transmission and receiving will stop as a result. Likewise, the **undo t1 shutdown** command can bring up all these serial interfaces.

Example # Shut down the first T1 line on interface T3 2/0.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 shutdown
```

t1 unframed

Syntax **t1** *line-number* **unframed**

undo t1 *line-number* **unframed**

View CT3 interface view

Parameter *line-number*: T1 line number in the range 1 to 28.

Description Use the **t1 unframed** command to set a T1 line on the CT3 interface to work in unframed mode (T1 mode).

Use the **undo t1 unframed** command to set the T1 line on the CT3 interface to work in framed mode (CT1 mode).

By default, T1 lines are working in framed mode.

A T1 line in unframed mode does not contain the frame control information; it cannot be divided into timeslots. For it, the system automatically creates a serial interface numbered **serial** *number***/***line-number***:0**. This interface operates at 1544 kbps and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Related command: **t1 channel-set**.

Example # Set the first T1 line on interface T3 2/0 to work in unframed mode.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] t1 1 unframed
```

using (CT3 interface view)

Syntax **using** { **ct3** | **t3** }

View CT3 interface view

Parameter **ct3**: Sets the CT3 interface to operate in channelized mode.

t3: Sets the CT3 interface to operate in unchannelized mode.

Description Use the **using** command to configure the operating mode of a CT3 interface.

Use the **undo using** command to restore the default, that is, channelized mode.

You can configure T1 lines on CT3 interfaces operating in channelized mode only.

When a CT3 interface operates in unchannelized mode, the system automatically creates a serial interface numbered **serial** *number***/0:0** for it. This interface operates at 44.736 Mbps and is logically equivalent to a synchronous serial interface on which you can make other configurations.

Example # Configure interface T3 2/0 to operate in unchannelized mode.

```
<Sysname> system-view
[Sysname] interface t3 2/0
[Sysname-T3 2/0] using t3
```

18 ISDN BRI INTERFACE CONFIGURATION COMMANDS

loopback (ISDN BRI interface view)

Syntax **loopback { b1 | b2 | both }**

undo loopback

View ISDN BRI interface view

Parameter **b1**: Places the B1 channel in external loopback.

b2: Places the B2 channel in external loopback.

both: Places both B1 and B2 channels in external loopback.

Description Use the **loopback** command to sets the B1, B2, or both channels on the ISDN BRI interface in external loopback. This can send data from a line back to the line.

Use the **undo loopback** command to restore the default.

By default, loopback is disabled on ISDN BRI interfaces.

CAUTION: *The modules with loopback-supported ISDN interfaces include 4BS (MIM), and 1BS1BU2BS2BU (SIC). In addition, loopback is also supported by the fixed ISDN interfaces on your router, if there is any.*

Example # Place the B1 and B2 channels on interface BRI 1/0 in external loopback.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] loopback both
```

19 ATM CONFIGURATION COMMANDS

atm class

Syntax **atm class** *atm-class-name*

undo atm class *atm-class-name*

View System view

Parameter *atm-class-name*: Name of ATM class, a string of 1 to 16 characters.

Description Use the **atm class** command to create an ATM class and enter the ATM class view.

Use the **undo atm class** command to delete the specified ATM class.

An ATM class is a group of predefined parameters that can be used for ATM interface or PVC.

Related command: **atm-class**.

Example # Create an ATM class named "main" and enter ATM class view.

```
<Sysname> system-view
[Sysname] atm class main
[Sysname-atm-class-main]
```

atm-class

Syntax **atm-class** *atm-class-name*

undo atm-class

View ATM interface view/PVC view

Parameter *atm-class-name*: Name of ATM class, a string of 1 to 16 characters.

Description Use the **atm-class** command to apply an ATM class to an ATM interface or a PVC.

Use the **undo atm-class** command to remove the ATM class applied to a ATM interface or a PVC.

Related command: **atm class**.

Example # Apply the ATM class named "main" to ATM 1/0 interface.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] atm-class main
```

atm-link check

Syntax **atm-link check**

undo atm-link check

View ATM P2P sub-interface view

Parameter None

Description Use the **atm-link check** command to have the protocol state of the ATM P2P sub-interface change depending on whether the physical interface is up and whether a PVC is configured on the sub-interface. The protocol of the sub-interface, which comes down otherwise, goes up when the physical interface is up and a PVC is configured on the sub-interface.

Use the **undo atm-link check** command to restore the default.

By default, the protocol of the ATM P2P sub-interface goes up or comes down depending on whether the physical interface is up or down.

This command applies only to ATM P2P sub-interfaces.

Example # Enable the protocol state of ATM P2P sub-interface 4/0.1 to change depending on whether the physical interface is up and whether a PVC is configured on the sub-interface.

```
<Sysname> system-view
[Sysname] interface atm 4/0.1 p2p
[Sysname-Atm4/0.1] atm-link check
```

clock

Syntax **clock** { **master** | **slave** }

undo clock

View ATM main interface view

Parameter *master*: Specifies the internal transmission clock.

slave: Specifies the line clock.

Description Use the **clock** command to specify the clock signal to be adopted by an ATM interface.

Use the **undo clock** command to restore the default.

By default, ATM interface uses line clock signal (slave). This clock signal is usually provided by device which provides ATM interfaces.

When two network devices are connected back-to-back through their ATM interfaces, you need to configure one interface to adopt the signal of the internal transmission clock.

The effect of this command applies to both ATM main interface and sub-interface. However, the command is available only in ATM main interface view.

Related command: **display atm interface**.

Example # Specify ATM 1/0 interface to adopt the signal of the internal transmission clock.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] clock master
```

display atm class

Syntax **display atm class** [*atm-class-name*]

View Any view

Parameter *atm-class-name*: ATM class name, a string of 1 to 16 characters.

Description Use the **display atm class** command to display the information about an ATM class.

Note that:

- If you provide the *atm-class-name* argument, this command displays the information about the ATM class identified by the argument.
- If you do not specify the *atm-class-name* argument, this command displays the information about all the ATM classes.

Example # Display the information about the ATM class named "main".

```
<Sysname> display atm class main
ATM CLASS: main
Service ubr 8000
encapsulation aal5snap
```

Table 23 Description on the fields of the display atm class command

Field	Description
ATM CLASS	ATM class name

Table 23 Description on the fields of the display atm class command

Field	Description
Service ubr 8000	The PVC's service type and the bit rate
encapsulation aal5snap	The type of ATM AAL5 encapsulation of the PVC is aal5snap.

display atm interface

Syntax **display atm interface** [**atm** *interface-number*]

View Any view

Parameter *interface-number*: Specifies an ATM interface to view the detailed information about.

Description Use the **display atm interface** command to display detailed information about ATM interface.

Note that:

If you provide the *interface-number* argument, this command displays the information about the ATM interface identified by the argument.

If you do not provide the argument, this command displays the information about all the ATM interfaces.

Example # Display the information about ATM 4/0 interface.

```
<Sysname> display atm interface atm 4/0
ATM interface Atm4/0, State UP
  Port Information:
    Maximum VCs: 1024
    PVCs: 5, MAPs: 1
    input pkts: 11603, input bytes: 426476, input pkt errors: 37092
    output pkts: 14053, output bytes: 519106, output pkt errors: 0
  Main interface Information:
    PVCs: 4, MAPs: 1
    input pkts: 11603, input bytes: 426476, input pkt errors: 19210
    output pkts: 14053, output bytes: 519106, output pkt errors: 0

ATM interface Atm4/0.1, point-to-point, State UP
  Sub-interface Information:
    PVCs: 1, MAPs: 0
    input pkts: 0, input bytes: 0, input pkt errors: 17880
    output pkts: 0, output bytes: 0, output pkt errors: 0
```

Table 24 Description on the fields of the display atm interface command

Field	Description
ATM interface Atm6/0/0, State UP	Name and state of the interface
Maximum VCs	Maximum number of VCs on the ATM interface

Table 24 Description on the fields of the display atm interface command

Field	Description
PVCs	Number of PVCs configured on the interface
MAPs	Number of maps on the interface
input pkts: 0, input bytes: 0, input pkt errors: 0	Received packets, bytes, and errors
output pkts: 69, output bytes: 2218, output pkt errors: 8	Transmitted packets, bytes, and errors

display atm map-info

Syntax **display atm map-info** [**interface** *interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

pvc-name: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI value pair. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

Description Use the **display atm map-info** command to view the map information on an ATM interface.

Note that:

- Without an interface specified, the system displays the map information for all ATM interfaces.
- Without specifying the PVC name or the VPI/VCI value pair, the system displays the map information of all PVCs on the specified ATM interface.

Example # Display map information for all ATM interfaces.

```
<Sysname> display atm map-info
Atm1/0, PVC 1/32, PPP, Virtual-Template10, UP
Atm1/0, PVC 1/33, IP & Mask, State UP
100.11.1.1, mask 255.255.0.0, vlink 1
Atm1/0, PVC 2/101, ETH, Virtual-Ethernet1, UP
```

Table 25 Description on the fields of the display atm map-info command

Field	Description
Atm1/0	Interface number
PVC 1/33	PVC identifier

Table 25 Description on the fields of the display atm map-info command

Field	Description
IP & Mask	Protocol type
State UP	Map entry state
100.11.1.1, mask 255.255.0.0	Protocol address
Vlink 1	Virtual link number

display atm pvc-group

Syntax **display atm pvc-group** [**interface** *interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

pvc-name: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI value pair. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

Description Use the **display atm pvc-group** command to view the information about PVC-Group.

Note that:

- If no interface is specified, the system displays PVC-Group information on all ATM interfaces.
- If the PVC name or the VPI/VCI value pair is not specified, the system displays information of all PVC-Groups on the specified ATM interface.

Example # Display the information about PVC-Group on all ATM interfaces.

```
<Sysname> display atm pvc-group
VPI/VCI   PVC-NAME      STATE ENCAP PROT     INTERFACE         GROUP
1/32           aa       UP    SNAP  IP     Atm11/0(UP)       1/32
1/33                    UP    SNAP  IP     Atm11/0(UP)       1/32
3/34                    UP    SNAP  IP     Atm11/0(UP)       1/32
```

Table 26 Description on the fields of the display atm pvc-group command

Field	Description
VPI/VCI	VPI/VCI value pair
PVC-NAME	PVC name
STATE	PVC state

Table 26 Description on the fields of the display atm pvc-group command

Field	Description
ENCAP	AAL5 encapsulation type of the PVC
PROT	Upper protocol running on the PVC
INTERFACE	Interface to which the PVC belongs
GROUP	PVC group to which the PVC belongs

display atm pvc-info

Syntax **display atm pvc-info** [**interface** *interface-type interface-number* [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]

View Any view

Parameter *interface-type interface-number*: Interface type and number.

pvc-name: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI value pair. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

Description Use the **display atm pvc-info** command to view the information about PVC.

Note that:

- Without an interface specified, the system displays PVC information on all ATM interfaces.
- Without a PVC name or a VPI/VCI value pair specified, the system displays all the PVC information on the specified ATM interface.

Example # Display the PVC information on all ATM interfaces.

```
<Sysname> display atm pvc-info
VPI/VCI | STATE   | PVC-NAME  | INDEX  | ENCAP  | PROT | INTERFACE
--------|---------|-----------|--------|--------|------|----------
1/32    |UP       |aa         |33      |SNAP    |IP    |Atm1/0 (UP)
1/33    |UP       |Sysname    |34      |MUX     |None  |Atm1/0 (UP)
1/55    |UP       |datacomm   |56      |SNAP    |PPP   |Atm1/0.1 (UP)
2/66    |UP       |           |68      |SNAP    |IP    |Atm1/0.4 (UP)
2/101   |UP       |beijing    |103     |SNAP    |ETH   |Atm1/0.2 (UP)
```

Table 27 Description on the fields of the display atm pvc-info command

Field	Description
VPI/VCI	VPI/VCI value pair
STATE	PVC state

Table 27 Description on the fields of the display atm pvc-info command

Field	Description
PVC-NAME	PVC name
INDEX	Internal index of the PVC
ENCAP	AAL5 encapsulation type of the PVC
PROT	Upper protocol running on the PVC
INTERFACE	Interface to which the PVC belongs

encapsulation

Syntax **encapsulation** *aal5-encap*

undo encapsulation

View PVC view/ATM Class view

Parameter *aal5-encap*: AAL5 encapsulation type; its possible values are as follows:

- aal5mux: MUX encapsulation type
- aal5nlpid: RFC1490 encapsulation type
- aal5snap: LLC/SNAP (logical link control/subnet access protocol) encapsulation type

Description Use the **encapsulation** command to specify ATM AAL5 encapsulation type for PVC.

Use the **undo encapsulation** command to restore the default.

By default, aal5snap encapsulation is adopted.

Note that:

- Among aal5snap, aal5mux and aal5nlpid, only aal5snap encapsulation supports InARP.
- If InARP is enabled, you need to disable it before change AAL5 encapsulation to aal5mux or aal5nlpid.
- An ATM PVC can carry multiple protocols simultaneously, but certain types of encapsulations may not support some applications (one or more of IPoA, IPoEoA, PPPoA and PPPoEoA). When such cases occur, the system gives a prompt.

Example # Specify the AAL5 encapsulation of PVC 1/32 on ATM 1/0 interface to aal5snap.

```
<Sysname>system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/32
[Sysname-atm-pvc-Atm1/0-1/32] encapsulation aal5snap
```

interface atm

Syntax **interface atm** { *interface-number* | *interface-number.subnumber* [**p2mp** | **p2p**] }

undo interface atm *interface-number.subnumber*

View System view

Parameter *interface-number*: ATM main interface number.

subnumber: ATM sub-interface number, in the range 0 to 1023.

p2mp: Point-to-multiple point connection on the sub-interface

p2p: Point-to-point connection on the sub-interface

Description Use the **interface atm** command to create an ATM sub-interface or enter an ATM sub-interface view

Use the **undo interface atm** command to delete ATM sub-interface.

Be default, the connection type of sub-interface is p2mp.

Two types of connections are available on ATM sub-interface: p2mp and p2p. In p2mp connection, you can create multiple PVCs on the sub-interface; In p2p connection, you can create just one PVC on the sub-interface.

]Example # Enter Atm1/0 interface.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0]
```

Create and enter sub-interface Atm1/0.1, and set its connection type to p2p.

```
<Sysname> system-view
[Sysname] interface atm 1/0.1 p2p
[Sysname-Atm1/0]
```

ip-precedence

Syntax **ip-precedence** { *pvc-name* [*vpi/vci*] | *vpi/vci* } { *min* [*max*] | **default** }

undo ip-precedence { *pvc-name* [*vpi/vci*] | *vpi/vci* }

View ATM PVC-group view

Parameter *pvc-name*: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI pair value. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

min: Minimum precedence of IP packets carried by the PVC, in the range 0 to 7.

max: Maximum precedence of IP packets carried by the PVC, in the range 0 to 7.

default: Uses the specified PVC as the default PVC.

Description Use the **ip-precedence** command to let different PVCs in PVC-group carry IP packets of different precedence levels.

Use the **undo ip-precedence** command to delete the precedence configuration of IP packets carried over PVC.

- If the **ip-precedence** command is not configured, all IP packets, regardless of their precedence levels, are transmitted over the primary PVC (the one used when the PVC-group is created) in the PVC-group.
- If this command is configured and the **default** keyword is used, which means the current PVC is set as the default PVC, then all the IP packets without specified precedence levels will be transmitted over this PVC.
- If this command is used without using the **default** keyword, which means no PVC is taken as the default PVC, all IP packets without specified precedence levels are transmitted over the primary PVC.
- This command is for configuration of the PVCs in the PVC-Group only. The specified minimum preference *min* should be not greater than the specified maximum preference *max*.

Note that this command does not change the precedence levels of IP packets.

Related command: **pvc-group**, **pvc**.

Example # Configure a PVC named "aa", whose VPI/VCI is 1/32, to carry IP packets with precedence level 0 to 3.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc-group aa 1/32
[Sysname-atm-pvc-group-Atm1/0-1/32-aa] ip-precedence aa 1/32 0 3
```

map bridge

Syntax **map bridge virtual-ethernet** *interface-number*

undo map bridge

View PVC view/ATM Class view

Parameter *interface-number*: Virtual Ethernet (VE) interface number.

Description Use the **map bridge** command to establish the IPoEoA mapping or PPPoEoA mapping on the PVC.

Use the **undo map bridge** command to delete the mapping.

By default, no mapping is configured.

Before using this command, make sure that the VE has been created.

Example The following example demonstrates a complete process of IPoEoA configuration.

Establish a VE interface virtual-Ethernet 1.

```
<Sysname> system-view
[Sysname] interface virtual-ethernet 1
```

Configure an IP address 10.1.1.1/16 for the VE interface.

```
[Sysname-Virtual-Ethernet1] ip address 10.1.1.1 255.255.0.0
[Sysname-Virtual-Ethernet1] quit
```

Create PVC 1/102 on the ATM interface Atm2/0

```
[Sysname] interface atm 2/0
[Sysname-Atm2/0] pvc 1/102
```

Establish the IPoEoA mapping using the established VE interface in PVC view.

```
[Sysname-atm-pvc-Atm2/0-1/102] map bridge virtual-ethernet 1
```

map ip

Syntax In PVC view:

map ip { *ip-address* [*ip-mask*] | **default** | **inarp** [*minutes*] } [**broadcast**]

undo map ip { *ip-address* | **default** | **inarp** }

In ATM class view:

map ip inarp [*minutes*] [**broadcast**]

undo map ip inarp

View PVC view, ATM class view

Parameter *ip-address*: Remote IP address mapped to PVC.

ip-mask: IP address mask. It specifies a network segment together with the *ip-address* argument. This allows the device to forward an IP packet out of the

PVC so long as a next-hop address in the specified network segment is found for the packet.

default: A mapping with the default route property is set. If a packet cannot find a mapping with the same address of next hop at the interface, but one PVC has the default mapping, the packet can be sent over the PVC.

inarp: Enables inverse address resolution protocol (InARP) on PVC.

minutes: Time interval to send InARP packets, in minutes. The value ranges from 1 to 600 and defaults to 15 minutes.

broadcast: Enables pseudo-broadcast. If a map of the PVC is configured with pseudo-broadcast, the device sends on the PVC a copy of each broadcast or multicast packet that it sends out the interface to which the PVC belongs.

You must configure the **broadcast** keyword on an ATM PVC where broadcast or multicast packets must be sent, for example, to allow PIM multicast to create neighbor relationship with the router connected using the ATM interface.

Description Use the **map ip** command to create IPoA mapping for PVC.

Use the **undo map ip** command to delete the mapping.

By default, no mapping is configured. If a mapping is configured, pseudo-broadcast is not supported by default.

Before configuring InARP, make sure the aal5snap encapsulation is used. InARP is not supported when using aal5mux or aal5nlpid encapsulations.

Example # Create a static mapping on PVC 1/32, specifying the opposite IP address to 61.123.30.169 and supporting pseudo-broadcast.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/32
[Sysname-atm-pvc-Atm1/0-1/32] map ip 61.123.30.169 broadcast
```

Enable InARP on PVC 1/33 and send InARP packets every 10 minutes.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/33
[Sysname-atm-pvc-Atm1/0-1/33] map ip inarp 10
```

map ppp

Syntax **map ppp virtual-template** *vt-number*

undo map ppp

View PVC view/ATM Class view

Parameter *vt-number*: Number of the virtual template (VT) interface corresponding to a PPPoA map.

Description Use the **map ppp** command to create a PPPoA map on the PVC.

Use the **undo map ppp** command to delete the map.

By default, no mapping is configured.

Before this command is used, the VT must have already been created.

Example The following example demonstrates a complete process of PPPoA configuration.

Create a VT interface numbered 10, and assign it an IP address.

<Sysname> system-view

```
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10] ip address 202.38.160.1 255.255.255.0
[Sysname-Virtual-Template10] quit
```

Create PVC 1/101 on interface Atm1/0.

```
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/101
```

Create a PPPoA map using the VT interface created.

```
[Sysname-atm-pvc-Atm1/0-1/101] map ppp virtual-template 10
```

mtu

Syntax **mtu** *mtu-number*

undo mtu

View Interface view

Parameter *mtu-number*: MTU size on ATM interface, in range of 128 to 2000 bytes.

Description Use the **mtu** command to set the size of maximum transmission unit (MTU) on ATM interface.

Use the **undo mtu** command to restore the default.

By default, the MTU of an ATM interface is 1,500 bytes.

The MTU only influences the packet assembly and disassembly at IP layer at the ATM interface. Due to the limit of QoS queue length (for example, the default length of the FIFO queue is 75), MTU which is too small may cause numerous fragments and thus be dropped by the QoS queue. In this case, the length of the QoS queue can be increased appropriately. The default queue dispatching

mechanism used by PVC is FIFO. You can use the **fifo queue-length** command in the PVC view to change its queue length.

The effect of this command applies to ATM main interface and sub-interface simultaneously.

Example # Set the MTU of ATM interface atm 1/0 to 1492 bytes.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] mtu 1492
```

oam ais-rdi

Syntax **oam ais-rdi up** *up-count* **down** *down-count*

undo oam ais-rdi

View PVC view, ATM class view

Parameter *up-count*: Period (in seconds). A PVC goes up if no alarm indication signal/remote defect indication (AIS/RDI) alarm cell is received in the period specified by this argument. The value range of this argument varies with device model.

down-count: Number of AIS/RDI alarm cells. A PVC goes down if the number of the successive AIS/RDI alarm cells received reaches the number specified by this argument. The value range of this argument varies with device model.

Description Use the **oam ais-rdi** command to modify the parameters related to AIS/RDI alarm cell detection.

Use the **undo oam ais-rdi** command to restore the default.

By default, AIS/RDI alarm cell detection is enabled, which means a PVC goes down if the number of successive AIS/RDI alarm cells received reaches that specified by the *down-count* argument, and it goes up if no AIS/RDI alarm cell is received in a period specified by the *up-count* argument.

Note that the **oam ais-rdi** command is not applicable to the secondary PVCs of a PVC group.

- *The primary PVC of a PVC group is the PVC based on which the PVC group is created.*
- *Second PVCs are created in PVC groups.*

Example # Configure the AIS/RDI alarm detection parameters for PVC 1/32, setting both *up-count* and *down-count* to 5.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/32
[Sysname-atm-pvc-Atm1/0-1/32] oam ais-rdi up 5 down 5
```

oam frequency

Syntax **oam frequency** *frequency* [**up** *up-count* **down** *down-count* **retry-frequency** *retry-frequency*]

undo oam frequency

View PVC view/ATM Class view

Parameter *frequency*: Time interval to send operations, administration, and maintenance (OAM) F5 Loopback cells, in seconds, and the range of the value is 1 to 600.

up-count: Number of OAM F5 Loopback cells. A PVC goes up only when the number of the OAM F5 Loopback cells successively and correctly received reaches the number specified by this argument. This argument ranges from 1 to 600. The system default is 3.

down-count: Number of OAM F5 Loopback cells. A PVC goes down only when the number of the successive OAM F5 Loopback cells not received reaches the number specified by this argument. This argument ranges from 1 to 600. The system default is 5.

retry-frequency: Interval (in seconds) to send OAM F5 Loopback cell in retransmission detection before PVC status changes. This argument ranges from 1 to 1,000. The system default is 1.

Description Use the **oam frequency** command to enable the transmission and retransmission detection of OAM F5 Loopback cell, as well as to modify the related parameters.

Use the **undo oam frequency** command to disable the transmission and retransmission detection of the cell.

By default, OAM F5 Loopback cell transmission is disabled, but if an OAM F5 Loopback cell is received, it should be responded.

The **oam frequency** command is not applicable to the secondary PVCs of a PVC group.

Example # Enable OAM F5 Loopback detection on PVC 1/32, with the period of 12 seconds. And set the retransmission detection *up-count* as 4, *down-count* as 4 and retransmission period as 1 second.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/32
[Sysname-atm-pvc-Atm1/0-1/32] oam frequency 12 up 4 down 4 retry-frequency 1
```

oamping interface

Syntax **oamping interface atm** *interface-number* **pvc** { *pvc-name* | *vpi/vci* } [*number timeout*]

View ATM interface view

Parameter **atm** *interface-number*: ATM interface number.

pvc-name: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI pair value. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

number: Number of OAM cells to be transmitted consecutively, in the range 1 to 1,000. The system default is 5.

timeout: OAM response timeout period in seconds, in the range 1 to 30. The system default is 2.

Description Use the **oamping interface** command to send OAM cells over the specified PVC on the specified ATM interface so as to check the link state. If no response is received within the specified time, this means that the link is bad, or too busy that packets are lost.

Example # Check the link state of PVC 1/32 on ATM interface 1/0, sending three cells and setting timeout period to one second.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] oamping interface atm 3/0 pvc 1/32 3 1
  Ping interface Atm3/0,pvc 0/45, with 5 of 53 bytes of ATM OAM F5 end-to-end
cell(s),
  timeout is 1 second(s), press CTRL_C to break
        Receive reply from pvc 1/32: time=1 ms
        Receive reply from pvc 1/32: time=1 ms
        Receive reply from pvc 1/32: time=1 ms
```

pvc

Syntax **pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }

undo pvc { *pvc-name* [*vpi/vci*] | *vpi/vci* }

View ATM interface view, PVC-Group view

Parameter *pvc-name*: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI pair value. For example, the name 1/20 is not allowed.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, VCI values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details regarding the value range, refer to Table 28.

Table 28 VCI range for each type of ATM interface

Interface type	VCI
ADSL	<0-255>
G.SHDSL	<0-255>
ATMOC3	<0-1023>
ATME3	<0-1023>
ATMT3	<0-1023>

- *The vpi and vci argument cannot both be 0.*
- *A PVC in a specific PVC-Group cannot be removed in ATM interface view.*

Description Use the **pvc** command to create a PVC or enter the PVC view on ATM interface, or to add the specified PVC into PVC-Group.

Use the **undo pvc** command to delete the specified PVC.

By default, no PVC is created.

- If you specified the *pvc-name* argument when creating a PVC, you can use the **pvc** *pvc-name* [*vpi/vci*] command to enter the view of that PVC
- You can use either the **undo pvc** *pvc-name* [*vpi/vci*] command or the **undo pvc** *vpi/vci* command to delete that PVC.

The VPI/VCI value of a PVC should be unique at an ATM interface (including the main interface and the sub-interface).

The actual number of PVCs that can be created depends on the **pvc max-number** command.

Related command: **display atm pvc-info**, **pvc max-number**.

Example # Create a PVC named "aa" with the VPI/VCI value of 1/101.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc aa 1/101
```

pvc-group

Syntax **pvc-group** { *pvc-name* [*vpi/vci*] | *vpi/vci* }

undo pvc-group { *pvc-name* [*vpi/vci*] | *vpi/vci* }

View ATM interface view

Parameter *pvc-name*: PVC name, a unique string of 1 to 16 characters on ATM interface, not case-sensitive. The name cannot be the same as a valid VPI/VCI pair value. For example, the name 1/20 is not allowed. The PVC corresponding to *pvc-name* must have already been created.

vpi/vci: VPI/VCI pair. VPI is short for virtual path identifier; its value ranges from 0 to 255. VCI is short for virtual channel identifier; its value range varies by interface type. Normally, values from 0 to 31 are reserved for special purpose, you are not recommended to use them. For details on the value range, refer to "VCI range for each type of ATM interface" on page 307.

Description Use the **pvc-group** command to create a PVC group or enter PVC group view.

Use the **undo pvc-group** command to delete the specified PVC-Group.

In creating a PVC-Group, the *pvc-name* argument or the *vpi/vci* argument defines the primary PVC of the PVC-Group.

Before creating a PVC group, make sure the corresponding PVC exists.

The **encapsulation** command and the oam-related commands are not applicable to secondary PVCs. The configurations corresponding to these commands on the primary PVC of a PVC group apply to all the secondary PVCs in the PVC group.

Related command: **ip-precedence**, **pvc**.

Example # Create a PVC group named "aa", with the primary PVC being the PVC with the VPI/VCI value of 1/32.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc aa 1/32
[Sysname-atm-pvc-group-Atm1/0-1/32-aa] quit
[Sysname-Atm1/0] pvc-group aa 1/32
```

pvc max-number

Syntax **pvc max-number** *max-number*

undo pvc max-number

View ATM interface view

Parameter *max-number*: Maximum number of PVCs allowed. The value range varies by the type of physical interface, as shown in the following table.

Table 29 The maximum number of PVCs supported on different types of ATM interfaces

Interface type	Maximum number	Default
ADSL	1 to 32	32
GSHDSL	1 to 32	32
ATM OC3	1 to 1,024	1,024
ATM25	1 to 256	256
ATME3	1 to 1,024	1,024
ATMT3	1 to 1,024	1,024

Description Use the **pvc max-number** command to set the maximum number of PVCs allowed on an ATM interface.

Use the **undo pvc max-number** command to restore the default.

The maximum number of PVCs allowed varies with interface type.

The maximum number specified in this command is the total number of the PVCs available to both ATM main interface and the sub-interfaces.

The effect of this command applies to both ATM main interface and sub-interface. However, the command itself is available only in ATM main interface view.

Example # Configure Atm 1/0 interface to support up to 1,024 PVCs.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc max-number 1024
```

pvp limit

Syntax **pvp limit** *vpi output-scr*

undo pvp limit *vpi*

View ATM interface view

Parameter *vpi*: Virtual path identifier of ATM network; its value ranges from 0 to 255.

output-scr: Sustainable rate of ATM cell output, in kbps. For its detailed value range, refer to Table 30.

Description Use the **pvp limit** command to set the parameters for VP policing.

Use the **undo pvp limit** command to delete the VP policing.

By default, VP policing is not performed.

When applying VP policing, the parameters of PVC are still valid. Only when the parameters of PVC and VP policing are satisfied, will the packets be transmitted and received. In calculating the traffic, the LLC/SNAP, MUX and NLPID headers are included, but the ATM cell head is not included.

Related command: **pvc**, **service cbr**, **service vbr-nrt**, **service vbr-rt**, **service ubr**.

Example # Set the traffic of VP with vpi 1 to 2M.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvp limit 1 2000
```

service cbr

Syntax **service cbr** *output-pcr* [**cdvt** *cdvt-value*]

View PVC view/ATM Class view

Parameter *output-pcr*: Output peak rate of ATM cell in kbps. The value range of this parameter varies with interface type, as shown in the following table

Table 30 Value ranges of output-pcr

Interface type	Value range of output-pcr
ADSL	64 to 640
G.SHDSL	For two-wire interfaces or four-wire interfaces in two-wire mode: 64 to 2,312
	For four-wire interfaces: 128 to 4,624
ATMOC3	64 to 155,000
ATME3	64 to 34,000
ATMT3	64 to 44,000

cdvt-value: cell delay variation tolerance, in μs. The effective range is 0 to 10,000 and the default is 500 μs. This argument cannot be configured in ATM Class view.

Description Use the **service cbr** command to specify PVC service type as constant bit rate (CBR).

By default, the service type is UBR after creating a PVC.

You can use this command to set the PVC service type and the rate parameter. The newly specified PVC service type will replace the existing service type. You are recommended to create the PVC with larger bandwidth first and then the one with smaller bandwidth. If the creation fails, you can increase the *cdvt-value* and try to create the PVC again. In the command line, the system will prompt you on this, as follows:

```
"fail to set service parameter, please adjust cdvt value"
```

The command is not applicable to ATM E1 interfaces and ATM E3 interfaces.

Related command: **service vbr-nrt**, **service vbr-rt**, **service ubr**.

Example # Create a PVC named "aa", with the VPI/VCI value of 1/101.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc aa 1/101
```

Specify the service type of the PVC as cbr and the peak rate of ATM cell as 50,000 kbps, and the cell delay variation tolerance as 1000 μs.

```
[Sysname-atm-pvc-Atm1/0-1/101-aa] service cbr 50000 cdvt 1000
```

service ubr

Syntax **service ubr** *output-pcr*

View PVC view/ATM Class view

Parameter *output-pcr*: Output peak rate of ATM cell in kbps. For the value ranges of this parameter, see Table 30.

Description Use the **service ubr** command to specify the service type of PVC as unspecified bit rate (UBR) and specify the related rate parameters.

By default, the service type is UBR after creating a PVC.

You can use this command as well as the **service vbr-nrt**, **service vbr-rt** and **service cbr** commands to set the service type and the rate-related parameters of a PVC. A newly configured PVC service type overwrites the existing one.

Related command: **service vbr-nrt**, **service vbr-rt**, and **service cbr**.

Example # Create a PVC named "a" with the VPI/VCI value of 1/101.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] service pvc aa 1/101
```

Specify the service type of the PVC as ubr and the peak cell rate of ATM cell as 100,000 kbps.

```
[Sysname-atm-pvc-Atm1/0-1/101-aa] service ubr 100000
```

service vbr-nrt

Syntax **service vbr-nrt** *output-pcr output-scr output-mbs*

View PVC view/ATM Class view

Parameter *output-pcr*: Peak rate of ATM cell output in kbps. For the value ranges of this parameter, see Table 30.

output-scr: Sustainable rate of ATM cell output in kbps. Its value ranges are the same as those of *output-pcr*.

output-mbs: Maximum burst size for ATM cell output, that is, the maximum number of ATM cells that the output interface can cache. The value ranges from 1 to 512.

Description Use the **service vbr-nrt** command to specify the service type of PVC as variable bit rate-non real time (VBR-NRT) and specify the related rate parameters.

By default, the service type is UBR after creating a PVC.

You can use this command as well as the **service ubr**, **service vbr-rt** and **service cbr** commands to set the service type and rate-related parameters of a PVC. A newly configured PVC service type overwrites the existing one.

Related command: **service ubr**, **service vbr-rt**, and **service cbr**.

Example # Create a PVC named "aa", with the VPI/VCI value of 1/101.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc aa 1/101
```

Specify the service type of the PVC as VBR-NRT and set the peak bit rate of ATM cell to 100,000 kbps, the sustainable bit rate to 50,000 kbps and the maximum burst size to 320 cells.

```
[Sysname-atm-pvc-Atm1/0-1/101-aa] service vbr-nrt 100000 50000 320
```

service vbr-rt

Syntax **service vbr-rt** *output-pcr output-scr output-mbs*

View PVC view/ATM Class view

Parameter *output-pcr*: Peak cell rate of ATM output in kbps. For the value ranges of this parameter, see Table 30.

output-scr: Sustainable cell rate of ATM output in kbps. Its value ranges are the same as those of *output-pcr*.

output-mbs: Maximum burst size of ATM cell output, that is, the maximum cache size of ATM cell output at the interface in cell number. The range of the value is 1 to 512. When it is used in ATM E3 interface, the range of the parameter is 1 to 512.

Description Use the **service vbr-rt** command to set the service type of PVC to Variable Bit Rate - Real Time (VBR-RT) and specify the related rate parameters in the PVC view.

By default, the service type is UBR after creating a PVC.

You can use this command as well as the **service ubr**, **service cbr** and **service vbr-nrt** commands to set the service type and rate-related parameters of a PVC. A newly configured PVC service type overwrites the existing one. This command is not applicable to ATM E1 interfaces.

Related command: **service vbr-nrt**, **service ubr**, and **service cbr**.

Example # Create a PVC named "aa" with the VPI/VCI value of 1/101.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc aa 1/101
```

Specify the service type of the PVC as VBR-RT and set the peak cell rate of ATM to 100,000 kbps, the sustainable cell rate to 50,000 kbps, and the maximum burst size to 320 cells.

```
[Sysname-atm-pvc-Atm1/0-1/101-aa] service vbr-rt 100000 50000 320
```

shutdown

Syntax **shutdown**

undo shutdown

View ATM interface view

Parameters None

Description Use the **shutdown** command to shut down an ATM interface.

Use the **undo shutdown** command to bring up an ATM interface.

By default, an ATM interface is up.

Examples # Shut down ATM 5/0.

```
<Sysname> system-view
[Sysname] interface Atm 5/0
[Sysname-Atm5/0] shutdown
```

Bring up ATM 5/0.

```
<Sysname> system-view
[Sysname] interface Atm 5/0
[Sysname-Atm5/0] undo shutdown
```

transmit-priority

Syntax **transmit-priority** *value*

undo transmit-priority

View PVC view

Parameter *value*: Transmission priority, in the range 0 to 9, the higher value indicating a higher priority.

The priority level for the UBR service ranges from 0 to 4.

The priority level for the VBR-NRT service ranges from 5 to 7.

The priority level for the VBR-RT service ranges from 8 to 9.

Description Use the **transmit-priority** command to assign transmission priority for an ATM PVC associated with the UBR, VBR-T, or VBR-NRT service. At the time of bandwidth allocation, the PVCs with higher priorities take precedence over those with lower priorities.

Use the **undo transmit-priority** command to restore the default transmission priority.

By default, the transmission priority of UBR service, VBR-NRT service, and VBR-RT service are 0, 5, and 8.

If you change the service type of a PVC, the transmission priority of the PVC changes to the default for the current service.

Example # Set the transmission priority of ATM PVC 1/32 to 3.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 1/32
[Sysname-atm-pvc-Atm1/0-1/32] transmit-priority 3
```

20 DCC CONFIGURATION COMMANDS

*Set all synchronous/asynchronous serial interfaces involved in DCC configuration to work in asynchronous mode with the **physical-mode async** command.*

dialer bundle

Syntax **dialer bundle** *number*

undo dialer bundle

View Dialer interface view

Parameter *number*: Dialer bundle number, in the range 1 to 255.

Description Use the **dialer bundle** command to associate a dialer bundle with a dialer interface in RS-DCC.

Use the **undo dialer bundle** command to remove the association.

By default, dialer interfaces are not associated with any dialer bundle in RS-DCC.

This command applies only to dialer interfaces. In addition, a dialer interface can be associated with only one dialer bundle.

Related command: **dialer bundle-member**.

Example # Associate dialer bundle 3 with interface Dialer1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer bundle 3
```

dialer bundle-member

Syntax **dialer bundle-member** *number* [**priority** *priority*]

undo dialer bundle-member *number*

View Dial (physical) interface view

Parameter *number*: Dialer bundle number, in the range 1 to 255.

priority *priority*: Priority of a physical interface in the dialer bundle. The *priority* argument is in the range 1 to 255. The higher the number, the higher the priority. The physical interface with higher priority is used first. The default priority is 1.

Description Use the **dialer bundle-member** command to assign a physical interface to a dialer bundle in RS-DCC.

Use the **undo dialer bundle-member** command to remove a physical interface from a dialer bundle.

By default, a dialer bundle contains no physical interface.

This command applies only to physical interfaces. A physical interface can belong to multiple dialer bundles.

Related command: **dialer bundle**.

Example # Assign interface BRI 1/0 to Dialer bundle 1 and Dialer bundle 2, with a priority of 50 in both.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] dialer bundle-member 1 priority 50
[Sysname-Bri1/0] dialer bundle-member 2 priority 50
```

dialer callback-center

Syntax **dialer callback-center** [**user** | **dial-number**] *

undo dialer callback-center

View Dial interface (physical or dialer) view

Parameter **user**: Sets the callback reference to user mode where DCC identifies which dial string is to be used for placing a return call by looking at the remote username configured in the **dialer route** command.

dial-number: Sets the callback reference to dial number mode, where DCC uses dial strings configured in **service-type ppp callback-number** commands in local user view to place return calls. When placing a return call, it needs to identify the dial string to be used by comparing the remote username obtained in PPP negotiation against the local user database for a match.

Description Use the **dialer callback-center** command to configure the PPP callback reference.

Use the **undo dialer callback-center** command to remove the setting.

By default, no PPP callback reference is configured.

This command is mandatory on the PPP callback server.

With both references configured, the device always attempts to place return calls in the user reference approach and in case failure occurs the dial number reference approach. If the command is configured with neither keyword, it equals the **dialer callback-center user dial-number** command.

Related command: **ppp callback** in *PPP Commands* in *Access Volume*.

Example # Specify the device as the PPP callback server, and set the callback reference to user mode.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] ppp callback server
[Sysname-Serial2/0] dialer callback-center user
[Sysname-Serial2/0] dialer route ip 1.1.1.2 user Sysnameb 8810052
```

Specify the device as the PPP callback server, and set the callback reference to dial number mode.

```
<Sysname> system-view
[Sysname] local-user usera
[Sysname-luser-usera] password simple usera
[Sysname-luser-usera] service-type ppp
[Sysname-luser-usera] service-type ppp callback-number 8810048
[Sysname-luser-usera] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp callback server
[Sysname-Serial2/0] dialer callback-center dial-number
```

dialer call-in

Syntax **dialer call-in** *remote-number* [**callback**]

undo dialer call-in *remote-number* [**callback**]

View Dial interface (physical or dialer) view

Parameter *remote-number*: Used for matching ISDN calling numbers. The asterisks (*) represent any characters.

callback: Enables the device to place a return call if an incoming number matches the number specified by the *remote-number* argument.

Description Use the **dialer call-in** command to configure a valid ISDN calling number and with the **callback** keyword to enable callback for the number.

Use the **undo dialer call-in** command to remove the setting.

By default, ISDN callback is disabled.

When receiving an incoming ISDN call, the device with the **dialer call-in** command configured first verifies that the caller is valid before processing the call. If the remote PBX does not provide the calling number, the call is dropped directly.

*On a dial interface (physical or Dialer) configured with the **dialer call-in** command, you need to configure the corresponding **dialer route** command or **dialer number** command, making sure that the dial-number configured in the command is the same as the remote-number configured in the **dialer call-in** command.*

Related command: **dialer callback-center**.

Example # Configure the device to place return calls for ISDN calling number 8810152.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] dialer route ip 100.1.1.2 8810152
[Sysname-Bri1/0] dialer call-in 8810152 callback
```

dialer circular-group

Syntax **dialer circular-group** *number*

undo dialer circular-group

View Dial interface (physical) view

Parameter *number:* Number of dialer circular group, same as the one defined in the **interface dialer** command. It ranges from 0 to 1023.

Description Use the **dialer circular-group** command to assign the physical interface to a dialer circular group in C-DCC approach.

Use the **undo dialer circular-group** command to remove the interface from the dialer circular group.

By default, a dialer circular group does not include any physical interfaces.

In C-DCC, you can assign a physical interface to a dialer interface by assigning it to the dialer circular group associated with the dialer interface. While a physical interface can belong to only one dialer interface, a dialer interface includes all physical interfaces assigned to its associated dialer circular group. When placing a call on the dialer interface, DCC selects the physical interface with higher priority.

Related command: **interface dialer**.

Example # Add interface Serial 2/0 and Serial 2/1 to dialer circular group 1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] quit
[Sysname] interface serial 2/0
```

```
[Sysname-Serial2/0] dialer circular-group 1
[Sysname-Serial2/0] quit
[Sysname] interface serial 2/1
[Sysname-Serial2/1] dialer circular-group 1
```

dialer disconnect

Syntax **dialer disconnect** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **dialer disconnect** command to clear the dialup link on an interface or all dialup links if no interface is specified.

Example # Clear the dialup link on interface Dialer0.

```
<Sysname> dialer disconnect interface dialer0
```

dialer enable-circular

Syntax **dialer enable-circular**

undo dialer enable-circular

View Dial interface (physical or dialer) view

Parameter None

Description Use the **dialer enable-circular** command to enable circular dial control center (C-DCC).

Use the **undo dialer enable-circular** command to disable C-DCC.

By default, C-DCC is enabled on ISDN BRI and PRI interfaces but disabled on other interfaces.

You need to enable C-DCC before you can use it.

To use resource-shared DCC (RS-DCC) on a dialer interface, you need to configure the **dialer user** command and the **dialer bundle** command on the dialer interface and assign physical interfaces to the dialer bundle with the **dialer bundle-member** command.

After you disable C-DCC, the system clears all configurations on dial interfaces. To make them recover, you need to shut down and then bring up them by performing the **shutdown** command and then the **undo shutdown** command.

If you perform the **dialer enable-circular** command or its **undo** form on a non-dial interface, do the same on the interface to recover it.

Related command: **dialer circular-group**.

Example # Enable C-DCC on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer enable-circular
```

dialer flow-interval

Syntax **dialer flow-interval** *interval*

undo dialer flow-interval

View System view

Parameter *interval*: Traffic statistics interval, in the range 1 to 1500 seconds.

Description Use the **dialer flow-interval** command to configure the traffic statistics interval for DCC.

Use the **undo dialer flow-interval** command to restore the default.

By default, the traffic statistics interval for DCC is 20 seconds.

This command is only useful for traffic-triggered dial in DCC. For example, when using traffic-triggered MP link bundling with DCC, you may need to configure DCC to send traffic statistics about dialup links at certain intervals to MP.

Related command: **dialer threshold**.

Example # Set traffic statistics interval to three seconds for DCC.

```
<Sysname> system-view
[Sysname] dialer flow-interval 3
```

dialer isdn-leased (physical interface view)

Syntax **dialer isdn-leased** *number*

undo dialer isdn-leased *number*

View Dial interface (Physical interface) view

Parameter *number*: Number of the ISDN B channel for leased line connection. It ranges from 0 to 1 for a BRI interface, and 0 to 30 (with 15 excluded for the control channel)

for a PRI interface, and 0 to 23 (with 23 excluded for the control channel) for a CT1/PRI interface.

Description Use the **dialer isdn-leased** command to configure an ISDN B channel for leased line connection.

Use the **undo dialer isdn-leased** command to remove the configuration.

By default, no ISDN B channel is configured to be leased line.

You may use any ISDN B channel for leased line connection without affecting other B channel settings.

On ISDN BRI interfaces, you may also configure ISDN BRI 128 kbps leased line. For more information, refer to the ***"dialer isdn-leased (ISDN BRI interface view)" on page 563****.*

Example # Configure the first B channel on interface BRI 2/0 as a leased line.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] dialer isdn-leased 0
```

dialer number

Syntax **dialer number** *dial-number*

undo dialer number

View Dial interface (physical or dialer) view

Parameter *dial-number:* Dial string for calling a remote end, a string of 1 to 30 characters.

Description Use the **dialer number** command to configure a dial number for placing calls to a single remote end.

Use the **undo dialer number** command to remove the configured dial string.

By default, no dial number is configured for calling the remote end.

You need to configure this command when the dialer or physical dial interface is the calling party.

In C-DCC, you may also use the **dialer route** command to configure multiple destination addresses or dial strings. In RS-DCC, however, you can only use the **dialer number** command to configure one dial string for each dialer interface, because associations between dialer interfaces and call destination address are one-to-one.

If no ***dialer-group*** *command is configured, DCC will not dial even if* ***dialer number*** *command is configured.*

Related command: **dialer route**.

Example # Set the dial string for placing calls to 11111 on interface Dialer1.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer number 11111
```

dialer priority

Syntax **dialer priority** *priority*

undo dialer priority

View Dial interface (physical) view

Parameter *priority*: Priority of the physical interface in a dialer circular group, in the range 1 to 127.

Description Use the **dialer priority** command to assign a priority to the physical interface in its dialer circular group in C-DCC approach.

Use the **undo dialer priority** command to restore the default.

By default, the priority of a physical interface in its dialer circular group is 1.

This command sets the order in which the available physical interfaces in a dialer circular group are used. The physical interface with higher priority is used first.

Related command: **dialer circular-group**.

Example # Set the priority of interface Serial 2/0 in dialer circular group 0 to 5.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer circular-group 1
[Sysname-Serial2/0] dialer priority 5
```

dialer queue-length

Syntax **dialer queue-length** *packets*

undo dialer queue-length

View Dial interface (physical or dialer) view

Parameter *packets*: Number of packets that can be buffered on the interface, in the range 1 to 100.

Description Use the **dialer queue-length** command to set the buffer queue length on the dial interface.

Use the **undo dialer queue-length** command to restore the default.

By default, no packets are buffered.

If no connection is available yet when a dial interface without a buffer queue receives a packet, it will drop the packet. Configured with a buffer queue, the dial interface will buffer the packet until a connection is available for packet sending.

Example # Set the buffer queue length to 10 on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer queue-length 10
```

dialer route

Syntax **dialer route** *protocol next-hop-address* [**mask** *network-mask-length*] [**broadcast** | **user** *hostname*] * [*dial-number*] [**autodial** | **interface** *interface-type interface-number*] *

undo dialer route *protocol next-hop-address* [**user** *hostname*] [**mask** *network-mask-length*] [*dial-number*] [**interface** *interface-type interface-number*]

View Dial interface (physical or dialer) view

Parameter *protocol*: Network protocol. At present, it can be **ip** only.

next-hop-address: IP address of dialed destination.

mask *network-mask-length*: Optional, mask length of the IP address of the dialed destination, in the range 0 to 32. If no mask length is specified, the default, 32, applies, where the *next-hop-address* argument is handled as a host address. If you want to set the *next-hop-address* argument to a network address, you must specify its mask length. Setting the *next-hop-address* argument to 0.0.0.0 and the *network-mask-length* argument to 0 indicates any next hop address. For example, the **dialer route ip 0.0.0.0 mask 0 8886** command indicates that you may call any IP address by dialing 8886.

user *hostname*: Remote username, a string of 1 to 80 characters used for authentication on incoming calls.

broadcast: Enables broadcast packets to pass through the link.

dial-number: Dial string for calling the remote end, a string of 1 to 30 characters.

autodial: If this keyword is used in a dialer route, you device will automatically attempt to dial according to the dialer route at certain intervals. The interval is set in the **dialer autodial-interval** command and defaults to 300 seconds.

interface *interface-type interface-number*: Specifies to dial from the specified physical interface. When multiple physical interfaces are assigned to a dialer interface and their dialup links are connected to different ISDN switches, you need to associate the dialup numbers with the physical interfaces. This configuration is intended for dialer interfaces in C-DCC only.

Description Use the **dialer route** command to enable a DCC interface to call the specified destination address (host or network address) or to receive calls from multiple remote ends.

Use the **undo dialer route** command to remove a dialer route.

To enable DCC to originate calls, you need to configure the *dial-number* argument.

If the **user** keyword is used, PPP authentication must be configured.

You may configure multiple dialer routes on a dial interface or for a destination address for the backup purpose.

*If the **dialer-group** command is not configured, DCC will not dial.*

Example # Dial 888066 to set up link for packets destined to network 192.168.1.0/24.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer route ip 192.168.1.0 mask 24 888066
```

Dial 888065 to set up link for packets destined to host address 192.168.1.1.

```
[Sysname-Serial2/0] dialer route ip 191.168.1.1 888065
```

dialer threshold

Syntax **dialer threshold** *traffic-percentage* [**in** | **in-out** | **out**]

undo dialer threshold

View Dialer interface view

Parameter *traffic-percentage*: Percentage of actual traffic on the link to bandwidth, in the range 0 to 99.

in: Considers only inbound traffic in actual load calculation.

in-out: Considers either inbound traffic or outbound traffic in actual load calculation, whichever is greater.

out: Considers only outbound traffic in actual load calculation.

Description Use the **dialer threshold** command to set the traffic threshold of a single link on the dialer interface. When the percentage of the traffic on the link to available bandwidth exceeds the threshold, another link is brought up to call the same destination address.

Use the **undo dialer threshold** command to restore the default.

By default, MP flow control is not enabled.

In DCC applications, you may configure load thresholds for links.

If you set a link load threshold in the range 1 to 99, MP tunes allocated bandwidth according to actual traffic percentage as follows:

- When the percentage of traffic on a link to bandwidth exceeds the defined traffic threshold, the system automatically brings up the second link, and assigns them to one MP bundle. When the percentage of traffic on these two links to bandwidth exceeds the defined traffic threshold, the system brings up the third link, and assigns it to the MP bundle, so on and so forth. This ensures appropriate traffic distribution on DCC links.
- On the contrary, when the percentage of the traffic on N (which is an integer greater than 2) links to the bandwidth of N - 1 links decreases under the defined traffic threshold, the system automatically shuts down a link, so on and so forth. This ensures the efficient use of DCC links.

If you set the link load threshold to zero, DCC brings up all available links when triggered by auto-dial or packets instead of looking at traffic size before doing that. In addition, the **dialer threshold 0** command voids the **dialer timer idle** command. DCC does not tear down links that has been established for timeout.

This command must be used in conjunction with the **ppp mp** command. To implement MP with DCC, you must use dialer interfaces.

Related command: **dialer flow-interval**.

Example # Set the link traffic threshold on interface Dialer1 to 80%.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer threshold 80
```

dialer timer autodial

Syntax **dialer timer autodial** *seconds*

undo dialer timer autodial

View Dial interface (physical or dialer) view

Parameter *seconds*: Interval before the next call attempt, in the range 1 to 604800 in seconds. The default interval is 300 seconds.

Description Use the **dialer timer autodial** command to set the auto-dial timer of DCC.

Use the **undo dialer timer autodial** command to restore the default.

By default, the auto-dial timer of DCC is 300 seconds.

This command takes effect only when the **auto-dial** keyword is configured in the **dialer route** command. It allows DCC to automatically dial at certain intervals to set up a connection. In the auto-dial approach, dial attempts to set up connection are not traffic triggered; once a connection is set up, it will not disconnect for idle-timeout. The use of auto-dial thus voids the **dialer timer idle** command.

Related command: **dialer route**.

Example # Set the auto-dial interval of DCC to 60 seconds on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer timer autodial 60
```

dialer timer compete

Syntax **dialer timer compete** *seconds*

undo dialer timer compete

View Dial interface (physical or dialer) view

Parameter *seconds*: Idle interval when contention occurs, in the range 0 to 65535 seconds.

Description Use the **dialer timer compete** command to set the compete-idle timer.

Use the **undo dialer timer compete** command to restore the default.

By default, the compete-idle timer is 20 seconds.

If all the channels are unavailable when DCC originates a new call, contention occurs.

Normally, an idle-timeout timer starts upon setup of a link. If a call to another destination address is placed at the same time, contention occurs. In this case, DCC starts a compete-idle timer to replace the idle-timeout timer for the link. When the idle time of the link reaches the setting of this compete-idle timer, the link disconnects.

Example # Set the compete-idle timer to 10 seconds on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer timer compete 10
```

dialer timer enable

Syntax **dialer timer enable** *seconds*

undo dialer timer enable

View Dial interface (physical or dialer) view

Parameter *seconds*: Holddown timer value, setting the interval for originating a call to bring up a link after it is disconnected. It ranges from 5 to 65535 seconds.

Description Use the **dialer timer enable** command to set the link holddown timer.

Use the **undo dialer timer enable** command to restore the default.

By default the link holddown timer is five seconds

A holddown timer starts upon disconnection of a link. The call attempt to bring up this link can be made only after the timer expires. This is to prevent a remote PBX from being overloaded.

To leave enough time for a server to call back, the interval between two calls on the client need to be at least 10 seconds longer than that of the server. It is recommended that the interval on the server be set to 5 seconds (the default) and that on the client be set to 15 seconds.

Example # Set the interval for DCC to make the next call attempt to 15 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer timer enable 15
```

dialer timer idle

Syntax **dialer timer idle** *seconds*

undo dialer timer idle

View Dial interface (physical or dialer) view

Parameter *seconds*: Link idle-timeout timer, setting the time that a link is allowed to be idle. It ranges from 0 to 65535 seconds.

Description Use the **dialer timer idle** command to set the link idle-timeout timer.

Use the **undo dialer timer idle** command to restore the default.

By default the link idle-timeout timer is 120 seconds

A link idle-timeout timer starts upon setup of a link. If no interesting packets are present before the timer expires, DCC disconnects the link.

If the timer is set to 0, the link will never be disconnected, regardless of whether there are interesting packets on the link or not.

Example # Set the link idle-timeout timer to 50 seconds on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer timer idle 50
```

dialer timer wait-carrier

Syntax **dialer timer wait-carrier** *seconds*

undo dialer timer wait-carrier

View Dial interface (physical or dialer) view

Parameter *seconds*: Wait-carrier timer value, setting the time waiting for call setup. This argument ranges from 0 to 65,535 (in seconds).

Description Use the **dialer timer wait-carrier** command to set the wait-carrier timer.

Use the **undo dialer timer wait-carrier** command to restore the default.

The wait-carrier timer defaults to 60 seconds.

Sometimes, the time that DCC waits for a connection to be established may vary call by call. To handle this situation, you may use a wait-carrier timer. A wait-carrier timer starts when a call is placed. If the connection is not established upon expiration of the timer, DCC terminates the call.

Example # Set the wait-carrier timer to 100 seconds on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer timer wait-carrier 100
```

dialer user

Syntax **dialer user** *username*

undo dialer user

View Dialer interface view

Parameter *username*: Remote username for PPP authentication, a string of 1 to 80 characters.

Description Use the **dialer user** command to add a remote username for authenticating incoming calls.

Use the **undo dialer user** command to remove the remote username.

By default, no remote username is set.

This command is only valid on dialer interfaces in RS-DCC.

On a dialer interface encapsulated with PPP, DCC identifies which dialer interface is to be used for receiving calls based on the remote username obtained through PPP authentication.

You may configure multiple dialer users (up to 255) on a dialer interface. This allows DCC to provide accesses to multiple dial interfaces by using one dialer interface.

Use this command on a C-DCC enabled dialer interface with caution. It enables RS-DCC and can remove the C-DCC configurations on the interface.

Performing the **undo dialer user** command on a dialer interface can clear all configurations on it.

Related command: **ppp pap local-user** on page 522 and **ppp chap user** on page 511.

Example # Add a remote username routerb.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] dialer user routerb
```

dialer-group

Syntax **dialer-group** *group-number*

undo dialer-group

View Dial interface (physical or dialer) view

Parameter *group-number*: Number of a dialer access group, in the range 1 to 255. You may define it with the **dialer-rule** command.

Description Use the **dialer-group** command to assign the interface to a dialer access group.

Use the **undo dialer-group** command to remove the interface from the dialer access group.

A DCC dial interface can belong to only one dialer access group. Configuring this command can overwrite the previous dialer access group setting for the interface, if any.

*In the default configuration of the interface, the **dialer-group** command is not configured. You must configure this command for DCC to send packets.*

Related command: **dialer-rule**.

Example # Add interface Serial 2/0 to dialer access group 1.

```
<Sysname> system-view
[Sysname] dialer-rule 1 acl 3101
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer-group 1
```

dialer-rule

Syntax **dialer-rule** *group-number* { *protocol-name* { **deny** | **permit** } | **acl** *acl-number* | **name** *acl-name* }

undo dialer-rule *group-number*

View System view

Parameter *group-number*: Number of a dialer access group, same as the *group-number* argument in the **dialer-group** command. It ranges from 1 to 255.

protocol-name: Network protocol, which can take **ip** or **ipx**.

deny: Denies packets of the specified protocol.

permit: Permits packets of the specified protocol.

acl *acl-number*: Specifies an ACL by its ACL number. The *acl-number* argument ranges from 2000 to 3999. An ACL number in the range 2000 to 2999 identifies a basic ACL; an ACL number in the range 3000 to 3999 identifies an advanced ACL.

name *acl-name*: Specifies an ACL by its name.

Description Use the **dialer-rule** command to set the condition for a DCC call to be placed for a dialer access group either by directly configuring a rule or by referencing an ACL.

Use the **undo dialer-rule** command to remove the setting.

You may configure a dial ACL to filter traffic that traverses a dial interface. Packets fall into two categories, depending on whether they are in compliance with the permit or deny statements in the dial ACL.

- Packets that match a permit statement or that do not match any deny statements. When receiving such a packet, DCC either sends it out if a link is present and resets the idle-timeout timer or originates a new call to set up a link if no link is present.
- Packets that do not match any permit statements or that match a deny statement. When receiving such a packet, DCC either sends it out without

resetting the idle-timeout timer if a link is present, or drops it without originating calls for link setup if no link is present.

For DCC to send packets normally, you must configure a dial ACL and associate it with the concerned dial interface (physical or dialer) by using the **dialer-group** command.

If no dial ACL is configured for the dialer access group associated with a dial interface, DCC will drop received packets on the interface as uninteresting ones.

Related command: **dialer-group**.

Example # Configure Dialer-rule1 and associate it with interface Serial 2/0.

```
<Sysname> system-view
[Sysname] dialer-rule 1 ip permit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] dialer-group 1
```

display dialer

Syntax **display dialer** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display dialer** command to display information about the specified or all DCC dial interfaces.

Example # Display information about all DCC dial interfaces.

```
<Sysname> display dialer
Dialer0 - dialer type = Dialer
   Dialer Route:
   NextHop_address          Dialer_Numbers
   Dialer number            003
   Dialer Timers(Secs):
   Autodial:300    Compete:20    Enable:5
   Idle:120    Wait-for-Carrier:60
   Total Channels:1  Free Channels:1
```

Table 31 Description on the fields of the display dialer command

Field	Description
dialer type	Type of dial interface, dialer or physical
NextHop address	Remote address associated with a dialer route on the interface
Dialer Number	Dial string for the remote IP address
Dialer Timers(Secs)	DCC timers
Auto-dial	Timer set by the **dialer timer autodial** command
Compete	Timer set by the **dialer timer compete** command

Table 31 Description on the fields of the display dialer command

Field	Description
Enable	Timer set by the **dialer timer enable** command
Idle	Timer set by the **dialer timer idle** command
Wait-for-carrier	Timer set by the **dialer timer wait-carrier** command
Total Channels	Total number of channels on the interface
Free Channels	Number of free channels

display interface dialer

Syntax **display interface dialer** [*number*]

View Any view

Parameters *number* : Dialer interface number.

Description Use the **display interface dialer** command to display the information about a dialer interface. If you do not provide this argument, this command displays the information about all the dialer interfaces.

Examples # Display the information about all the dialer interfaces.

```
<H3C> display interface dialer
Dialer1 current state: UP
Line protocol current state: UP (spoofing)
Description: Dialer1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is Dialer, baudrate: 64000 bps
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Length)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Table 32 Description on the fields of the display interface dialer command

Field	Description
current state	Physical state of a dialer interface (up/down)
Line protocol current state	Data link layer protocol state of the dialer interface (up/down)
Description	Interface description
The Maximum Transmit Unit	MTU of the dialer interface
Internet protocol processing	Network layer protocol state of the dialer interface (enabled/disabled)
Link layer protocol is PPP	Current data link layer protocol

Table 32 Description on the fields of the display interface dialer command

Field	Description
LCP initial	LCP is initialized.
Physical is Dialer	The physical interface is a dialer interface.
Output queue : (Urgent queuing : Size/Length/Discards)	Statistics on the packets in the urgent output queue
Output queue : (Protocol queuing : Length)	Statistics on the packets in the protocol output queue
Output queue : (FIFO queuing : Size/Length/Discards)	Statistics on the packets in the FIFO output queue
Last 300 seconds input: 0 bytes/sec, 0 packets/sec	Input interface data rate during the latest 300 seconds
Last 300 seconds output: 0 bytes/sec, 0 packets/sec	Output interface data rate during the latest 300 seconds
0 packets input, 0 bytes, 0 drops	Statistics on the packets reaching the interface
0 packets output, 0 bytes, 0 drops	Statistics on the packets sent through the interface

interface dialer

Syntax **interface dialer** *number*

undo interface dialer *number*

View System view

Parameter *number*: Dialer interface number, in the range 0 to 1023.

Description Use the **interface dialer** command to create a dialer interface. In C-DCC, this equals creating a dialer circular group.

Use the **undo interface dialer** command to remove a dialer interface.

By default, no dialer interface is created.

The dialer interface has a fixed baudrate of 64,000 bps.

In C-DCC, you may assign multiple physical interfaces to a dialer interface to inherit the attributes of this dialer interface by assigning them to the dialer circular group for the dialer interface with the **dialer circular-group** command. This is efficient where calling multiple destinations simultaneously is desired, because instead of configuring individual physical interfaces, you only need to configure multiple dialer routes on the dialer interface.

In RS-DCC, any dialer interface can use the services provided by multiple physical interfaces, and individual physical interfaces can provide services for multiple dialer interfaces at the same time. Therefore, authentication must be configured on these physical interfaces, so as to use the username of a dial-in party to locate the corresponding dialer interface for the call. In this mode, physical interfaces and dialer interfaces are dynamically bound. Furthermore, a dialer interface can only call a destination address as specified in the **dialer number** command.

The physical interfaces in C-DCC and Resource-Shared DCC do not use individual network addresses. Instead, they use the addresses of the corresponding dialer interfaces.

In both C-DCC and RS-DCC, physical interfaces use the network addresses of their associated dialer interface rather than being assigned separate addresses.

Example # Create dialer interface Dialer1.

```
<Sysname> system-view
[Sysname] interface dialer 1
```

ppp callback

Syntax **ppp callback** { **client** | **server** }

undo ppp callback { **client** | **server** }

View Dial interface (physical or dialer) view

Parameter **client**: Sends callback requests as the PPP callback client.

server: Accepts callback requests as the PPP callback server.

Description Use the **ppp callback** command to specify the interface as the server or client to send or accept PPP callback requests.

Use the **undo ppp callback** command to disable the interface as the PPP callback server or client.

By default, callback is disabled.

PPP callback adopts the client/server model where the calling party is the callback client and the called party is the callback server. The client first originates a call, and the server decides whether to originate a return call. If a return call is needed, the callback server disconnects and then originates a return call according to the information such as username or callback number.

This is useful for saving cost in the case that the call rates in two directions are different.

Example # Configure interface Serial 2/0 as the PPP callback server to accept callback requests.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp callback server
```

ppp callback ntstring

Syntax **ppp callback ntstring** *dial-number*

undo ppp callback ntstring

View Dial interface (physical or dialer) view

Parameter *dial-number*: Dial string for a Windows NT server to place return calls to your router, a string of 1 to 64 characters.

Description Use the **ppp callback ntstring** command to configure the dial number required for a Windows NT server to place return calls to your router.

Use the **undo ppp callback ntstring** command to remove the dial string.

By default, no callback dial string is configured for any Windows NT server.

When your router is functioning as a PPP callback client, configure this command if a Windows NT Server requires PPP callback clients to send callback numbers.

Related command: **ppp callback**.

Example # Set the dial string for a Windows NT server to call back the router to 1234567.

```
<Sysname> system-view
[Sysname] interface dialer 1
[Sysname-Dialer1] ppp callback ntstring 1234567
```

21 BASIC DLSW CONFIGURATION COMMANDS

code nrzi

Syntax **code nrzi**

undo code

View Synchronous serial interface view

Parameter None

Description Use the **code nrzi** command to configure the synchronous serial interface to use NRZI encoding.

Use the **undo code** command to configure the synchronous serial interface to use NRZ encoding.

By default, the NRZ encoding scheme is used on the synchronous serial interface.

There are two encoding schemes, NRZI and NRZ, for synchronous serial interface. The NRZ encoding scheme is generally used for synchronous serial interfaces of routers. The serial interfaces of some SNA devices, however, use NRZI encoding. Therefore, the encoding scheme of routers should be changed according to the encoding schemes used on the connected devices.

Example # Configure Serial 1/0 to use NRZI encoding.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] code nrzi
```

display dlsw circuits

Syntax **display dlsw circuits** [*circuit-id*] [**verbose**]

View Any view

Parameter *circuit-id*: Specifies the ID of a DLSw virtual circuit, in the range of 0 to 0xFFFFFFFF.

verbose: Displays the detailed information of the virtual circuits.

Description Use the **display dlsw circuits** command to view the DLSw virtual circuit information.

The output information of the command helps the user understand the condition of DLSw virtual circuits.

Example # Display the information of all virtual circuits.

```
<Sysname> display dlsw circuits
circuit-Id  port    local-MAC       remote-MAC      state       lifetime
00a2000a      04        0000.1738.6dfd  0000.1722.3435  CONNECTED   10:02:23
```

Table 33 Description on the fields of the display dlsw circuits command

Field	Description
circuit-Id	Virtual circuit ID
port	Port number used for TCP connection
local-MAC	The MAC address of the local peer across the virtual circuit
remote-MAC	The MAC address of the remote peer across the virtual circuit
State	Connection status. ■ CONNECTED: a TCP connection has been established ■ DISCONNECTED: no TCP connection has been established ■ CONNECTING: a TCP connection is being established
lifetime	The length of time for which the virtual circuit has been up

display dlsw information

Syntax **display dlsw information** [**local** | *ip-address*]

View Any view

Parameter **local**: Displays the local information about capabilities exchange.

ip-address: Specifies the IP address of the remote peer to display the capabilities exchange information about.

Description Use the **display dlsw information** command to display the DLSw capabilities exchange information.

The output information of the command helps the user to understand the condition of a DLSw virtual circuit.

Example # Display DLSw capabilities exchange information.

```
DLSw: Capabilities of local: 1.1.1.1   Vendor ID (OUI): 00.16.e0
  Version number       : 2         Release number      : 0
  Initial Pacing Window: 40        TCP sessions number : 1
  Multicast address    : None
  Version string       : 3Com OS software, Version 5.00c01 (Extended
), Release 1205, Standard
Copyright(c) 2004-2007 3Com Corporation and its licensors, All right
s reserved.
```

Table 34 Description on the fields of the display dlsw information command

Field	Description
DLSw	The IP address of the remote peer
Vendor ID(OUI)	The vendor ID of the remote device
Version number	The latest DLSw version currently supported by the remote device
Release number	Release version
Initial pacing window	Size of the initialized window
TCP sessions number	Number of TCP sessions
Multicast address	Multicast IP address configured on the remote device
Version string	Operating system version information of the remote peer

Display the local information about capabilities exchange.

```
DLSw: Capabilities of local: 1.1.1.1   Vendor ID (OUI): 00.0f.e2
  Version number       : 2         Release number      : 0
  Initial Pacing Window: 40        TCP sessions number : 1
  Multicast address    : None
  Version string       : Comware software, Version 5.20, Release 1205, Standard
  Copyright (c) 2004-2007 Hangzhou H3C Tech. Co., Ltd. All rights reserved.
```

display dlsw remote

Syntax **display dlsw remote** [*ip-address*]

View Any view

Parameter *ip-address*: Specifies the IP address of the remote peer to display the information about.

Description Use the **display dlsw remote** command to display the information of a remote peer or all remote peers.

With the *ip-address* argument provided, this command displays the information the specified remote DLSw peer; without the *ip-address* argument provided, this command displays the information all remote DLSw peers.

Example # Display information about all the current remote peers.

```
<Sysname> display dlsw remote
Remote peer type: D--Learning Dynamic
                  C--Configured by user
Total peers number:5
IP Address    frame-in  frame-out frame-drop  port  type  state
lifetime
*128.10.45.10     0          0          0         2065  C   CONNECT
00:00:00
128.10.46.78      2          2          0         2065  C   DISCONNECT
00:00:00
*130.20.45.12     2          2          0         2067      D   CONNECT
00:02:00
130.35.46.77      0          0          0         2067      C   DISCONNECT
00:00:00
```

```
*145.11.23.58     2          1          1         2067      C   CONNECTING
00:00:00
```

Table 35 Description on the fields of the display dlsw remote command

Field	Description
Remote peer type	Type of the remote peer ■ D: the remote peer was dynamically learned ■ C: the remote peer was manually configured
Total peers number	Total number of remote peers
IP address	Remote peer IP address (if preceded by a *, this remote peer can establish a connection; otherwise, this remote peer is inactive and only serves as a backup)
frame-in	Number of frames the local peer has received from this remote peer
frame-out	Number of frames the local peer has sent to this remote peer
frame-drop	Number of frames dropped due to errors while the local peer sent/received frames to/from this remote peer
port	Port number for the TCP connection ■ 2065: DLSw v1.0 ■ 2067: DLSw v2.0
type	Type of the remote peer
state	Status of the connection: ■ CONNECT: a TCP connection has been established ■ DISCONNECT: no TCP connection has been established ■ CONNECTING: a TCP connection is being established
lifetime	Length of time for which the connection has been up

display dlsw reachable-cache

Syntax **display dlsw reachable-cache**

View Any view

Parameter None

Description Use the **display dlsw reachable-cache** command to view the reachability information of DLSw.

Example # Display the reachability information of DLSw.

```
<Sysname> display dlsw reachable-cache
LOCAL MAC addresses in cache
------------------------------------------------------------------------
 MAC address       Status           Interface            Remain time

REMOTE MAC addresses in cache
------------------------------------------------------------------------
MAC address       Status          Peer       Type       Remain time
0102-2103-5641    FOUND           2.2.2.2    DYNAMIC    15
6500-7201-8160    FOUND           1.1.1.1    CONFIG     15
```

Table 36 Description on the fields of the display dlsw reachable-cache command

Field	Description
LOCAL MAC addresses in cache	Display the saved local reachability information
MAC address	MAC address of the terminal that is reachable to the local peer
Status	Status of the reachability information
Interface	The interface through which information destined to the MAC address will be sent
Remain time	Remaining aging time
REMOTE MAC addresses in cache	Display the saved remote reachability information
MAC address	MAC address of the terminal that is reachable to the remote peer
Status	Status of the reachability information
Peer	The remote peer to which the reachability information belongs
Type	Type of the reachability information ■ DYNAMIC: the information was dynamically learned ■ CONFIG: the information was manually configured
Remain time	Remaining aging time

display llc2

Syntax **display llc2** [**circuit** *circuit-id*]

View Any view

Parameter *circuit-id*: ID of an LLC2 virtual circuit, in the range of 0 to 4294967295.

Description Use the **display llc2** command to display LLC2 statistics.

Example # Display the statistics of the LLC2 virtual circuit by the ID of 46465025.

```
<Sysname> display llc2 circuit 46465025
llc2 circuit index 46465025
      Local   MAC  0.20.35.7b.e0.65
      Remote  MAC  0. 0.84.25.1e.e9
      Local   Sap  4
      Remote  Sap  4
      Role  secondary
      State : NORMAL
```

Table 37 Description on the fields of the display llc2 command

Field	Description
llc2 circuit index	Index of LLC2 circuit
Local MAC	Local MAC address of LLC2 circuit
Remote MAC	Remote MAC address of LLC2 circuit
Local Sap	Local SAP address of LLC2 circuit
Remote Sap	Remote SAP address of LLC2 circuit

Table 37 Description on the fields of the display llc2 command

Field	Description
Role	Local role of LLC2 circuit ■ primary" represents the end that initiated the circuit ■ secondary" represents the end accepted the circuit connection
State	State of the LLC2 circuit

dlsw bridge-set

Syntax **dlsw bridge-set** *bridge-set*

undo dlsw bridge-set *bridge-set*

View System view

Parameter *bridge-set*: ID of the bridge set to be mapped to DLSw, in the range of 1 to 63.

Description Use the **dlsw bridge-set** command to map the specified bridge set to DLSw.

Use the **undo dlsw bridge-set** command to remove mapping between the specified bridge set and DLSw.

By default, no bridge set is mapped to DLSw.

To enable forwarding frames of a bridge set to the remote end over a TCP connection, the local bridge set needs to be mapped to DLSw through this command. This command can be used repeated to map multiple bridge sets to DLSw.

For details about bridge set configuration, refer to "Bridging Configuration Commands" on page 549.

Example # Map the bridge set by the ID of 20 connected to DLSw.

```
<Sysname> system-view
[Sysname] bridge enable
[Sysname] bridge 20 enable
[Sysname] dlsw bridge-set 20
```

dlsw enable

Syntax **dlsw enable**

undo dlsw enable

View System view

Parameter None

Description Use the **dlsw enable** command to enable DLSw.

Use the **undo dlsw enable** command to disable DLSw.

By default, DLSw is enabled.

The execution of the **undo dlsw enable** command releases all dynamic resources without altering the configuration.

Example # Disable DLSw without changing the configuration.

```
<Sysname> system-view
[Sysname] undo dlsw enable
```

Enable DLSw.

```
<Sysname> system-view
[Sysname] dlsw enable
```

dlsw ethernet-frame-filter

Syntax **dlsw ethernet-frame-filter** *acl-number* { **inbound** | **outbound** }

undo dlsw ethernet-frame-filter { **inbound** | **outbound** }

View System view

Parameter *acl-number*: Layer 2 ACL number, in the range of 4000 to 4999.

inbound: Specifies to apply the ACL for inbound traffic.

outbound: Specifies to apply the ACL for outbound traffic.

Description Use the **dlsw ethernet-frame-filter** command to configure the DLSw router to filter Ethernet frames from or to the local SNA device by applying the specified ACL for inbound or outbound traffic.

Use the **undo dlsw ethernet-frame-filter** command to remove the ACL applied for the inbound or outbound traffic.

For more information about a Layer 2 ACL, refer to *"IPv4 ACL Configuration Commands" on page 2087* and *"IPv6 ACL Configuration Commands" on page 2103*.

Example # Apply ACL 4000 on the DLSw router to filter inbound Ethernet frames.

```
<Sysname> system-view
[Sysname] dlsw ethernet-frame-filter 4000 inbound
```

dlsw local

Syntax **dlsw local** *ip-address* [**init-window** *init-window-size* | **keepalive** *keepalive-interval* | **max-frame** *max-frame-size* | **max-window** *max-window-size* | **permit-dynamic** | **vendor-id** *vendor-id*] *

undo dlsw local *ip-address* [**init-window** | **keepalive** | **max-frame** | **max-window** | **permit-dynamic**] *

View System view

Parameter *ip-address*: IP address of the local peer to be created. This IP address must be reachable.

init-window-size: Initial local window size, in the range of 1 to 2,000. The default is 40 (frames).

keepalive-interval: Interval between keepalive messages, in seconds. The effective range is 0 to 1,200, and the default is 30 seconds. A value of 0 indicates that no keepalive message will be sent.

max-frame-size: Maximum frame size in bytes. Effective values include 516, 1,470, 1,500, 2,052, 4,472, 8,144, 11,407, 11,454, and 17,800, and the default is 1,500 bytes.

max-window-size: Maximum local window size, in the range of 1 to 2,000. The default is 50 (frames).

permit-dynamic: Permits non-peer routers to initiate connections to establish peering relationships dynamically with this router. It is not required to configure a remote peer for a router established as a local peer with this keyword included in the command.

vendor-id: DLSw vendor identifier, in the range of 00.00.00 to ff.ff.ff. The default is 00.e0.fc.

Description Use the **dlsw local** command to create a local DLSw peer.

Use the **undo dlsw local** *ip-address* command to remove the specified local DLSw peer.

Use the **undo dlsw local** *ip-address* { **init-window** | **keepalive** | **max-frame** | **max-window** | **permit-dynamic** } * command to restore the default parameters.

Deleting a local DLSw peer will automatically delete all its remote DLSw peers.

Establishing a TCP connection is the first step in establishing a DLSw circuit. To establish a TCP connection, you need to specify the IP addresses of both end systems across the TCP connection. By configuring a local DLSw peer, you specify the IP address of the local end across the TCP connection. This is required before a router can initiate or accept a TCP connection request. A router can only have one local peer.

Example # Create a local DLSw peer with the following parameters:

- IP address: 1.1.1.1
- Initial local window size: 50
- Keepalive interval: 40 seconds
- Maximum frame size: default
- Maximum local window size: default

```
<Sysname> system-view
[Sysname] dlsw local 1.1.1.1 init-window 50 keepalive 40
```

dlsw reachable

Syntax **dlsw reachable** { **mac-address** *mac-address* [**mask** *mask*] | **mac-exclusivity** | **saps** *saps-list* }

undo dlsw reachable { **mac-address** *mac-address* | **mac-exclusivity** | **saps** *saps-list* }

View System view

Parameter *mac-address*: Local reachable MAC address of the router, in the form of H-H-H.

mask: MAC address mask in the form of H-H-H, functionally similar to a subnet mask.

mac-exclusivity: Allows the router to access only those designated MAC addresses.

saps-list: List of local reachable SAP addresses of the router, in the form of *saps-list*=*saps-value*&<1-120>, where *saps-value* must be an even number in the range of 0x10 to 0xFE and &<1-120> means that you can specify up to 120 SAP addresses or SAP address ranges with this argument.

Description Use the **dlsw reachable** command to configure a local reachable MAC address or SAP addresses of the router.

Use the **undo dlsw enable** command to remove the reachability configuration.

After the **dlsw reachable** command is issued, the router notifies all connected routers of the local reachable MAC address or SAP addresses. Based on this information, the remote routers can decide whether to send frames to, without first polling, this router.

Note that you must change the configuration in time when changes occur to the local network.

Example # Permit access to MAC addresses that start with 1212.

```
<Sysname> system-view
[Sysname] dlsw reachable mac-address 1212-1212-1212 mask ffff-0000-0000
```

Allow the router to access SAP addresses 12 and 14.

```
[Sysname] dlsw reachable saps 12 14
```

Permit access to user-configured MAC addresses only.

```
[Sysname] dlsw reachable mac-exclusivity
```

dlsw reachable-cache

Syntax **dlsw reachable-cache** *mac-address* **remote** *ip-address*

undo dlsw reachable-cache *mac-address* **remote** *ip-address*

View System view

Parameter *mac-address*: MAC address of the SNA device connected to a remote peer.

ip-address: IP address of a remote peer.

Description Use the **dlsw reachable-cache** command to add the reachability information of the specified SNA device to the reachable-cache.

Use the **undo dlsw reachable-cache** command to remove the configured remote reachability information from the reachable-cache.

By default, no remote reachability information is configured.

This configuration allows the router to send frames to a remote peer without first polling it. When changes occur to the network of the remote peer, the configured reachability information needs to be updated.

Example # Add this remote reachability information to the reachable-cache: the IP address of the remote peer is 10.12.13.10, and the MAC address of the SNA device connected with it is 0102-2103-5641..

```
<Sysname> system-view
[Sysname] dlsw reachable-cache 0102-2103-5641 remote 10.12.13.10
```

dlsw remote

Syntax **dlsw remote** *ip-address* [**backup** *backup-address* | **keepalive** *keepalive-interval* | **linger** *minutes* | **max-frame** *max-frame-size* | **max-queue** *max-queue-length* | **priority** *priority*] *

undo dlsw remote *ip-address*

View System view

Parameter *ip-address*: IP address of the remote peer to be created.

backup *backup-address*: Creates a backup remote peer with the IP address of *ip-address*; *backup-address* is the IP address of the primary remote peer, which must be created prior to this backup remote peer.

keepalive-interval: Interval in seconds between keepalive messages, in the range of 0 to 1,200. The default is 30 seconds. A value of 0 indicates no keepalive will be sent.

minutes: Timeout time of the backup connection after the primary remote peer is disconnected, in units of minutes. The effective range is 0 to 1,440, and the default is 5 minutes. A value of 0 means that the backup remote peer will be kept connected after the primary remote peer is disconnected.

max-frame-size: Maximum frame size in bytes. Valid values include 516, 1,470, 1,500, 2,052, 4,472, 8,144, 11,407, 11,454, and 17,800. The default is 1,500 bytes.

max-queue-length: Size of the TCP input/output queue, in the range of 50 to 2,000. The default is 200.

priority: Transmission priority, in the range of 1 to 5. The default is 3.

Description

Use the **dlsw remote** command to create a remote DLSw peer.

Use the **undo dlsw remote** command to remove a remote peer.

After a local peer is created, a remote DLSw peer should be created to establish a TCP connection. The following command specifies the IP address of the remote router with which a TCP connection is to be established. After the configuration, the router will keep attempting to establish a TCP connection with the remote router. A router can have multiple remote peers.

Note that:

- Before creating a backup remote peer connection, make sure that a primary remote peer has been created.
- If a backup link exists after the primary link is disconnected from the TCP connection, the TCP link remains connected (you can see that a TCP connection exists by using the **display dlsw remote** command) until the backup link times out.

Example

Create a remote DLSw peer with the following parameters:

- IP address: 2.2.2.2
- Transmission priority: 2
- Keepalive interval: 40 seconds
- Maximum frame size: default
- Size of TCP input/output queue: 300

```
<Sysname> system-view
[Sysname] dlsw remote 2.2.2.2 priority 2 keepalive 40 max-queue 300
```

dlsw reverse

Syntax **dlsw reverse** *mac-address*

View System view

Parameter *mac-address*: MAC address to be converted.

Description Use the **dlsw reverse** command to convert a MAC address from the Ethernet format to the token ring format, or vice versa.

When specifying an SDLC peer MAC address for an SDLC virtual circuit, pay attention to the following situations:

- If the remote SNA device uses a token ring address, specify its MAC address directly.
- If the remote SNA device uses an Ethernet address, convert the Ethernet address to a token ring address by using the **dlsw reverse** command. For example, convert 00e0.fc03.a548 to 0007.3fc0.5a12.
- If the remote SNA device uses an SDLC link, specify a compound MAC address, in which the first five bytes are from the virtual MAC address configured in the **sdlc mac-map local** command on the remote router, and the last byte is the SDLC address of the local router.

Related command: **sdlc mac-map remote**.

Example # Convert the Ethernet format MAC address 0012-3578-4521 to the token ring format.

```
<Sysname> system-view
[Sysname] dlsw reverse 0012-3578-4521
Reversed MAC address: 0048-ac1e-a284
```

Convert the token ring MAC address 0048-ac1e-a284 to the Ethernet format.

```
[Sysname] dlsw reverse 0048-ac1e-a284
Reversed MAC address: 0012-3578-4521
```

dlsw max-transmission

Syntax **dlsw max-transmission** *retries*

undo dlsw max-transmission

View System view

Parameter *retries*: The maximum number of attempts that the DLSw v2.0 router should make to send an explorer frame. It ranges from 1 to 10 and defaults to 5.

Description Use the **dlsw max-transmission** command to set the maximum number of the attempts the DLSw v2.0 router should make to send an explorer frame.

Use the **undo dlsw max-transmission** command to restore the default.

Each time the origin DLSw v2.0 router sends an explorer frame in a UDP multicast or unicast, an explorer timer starts. If no acknowledgment is received before the explorer timer times out, the router retransmits the explorer frame and resets the explorer timer, until it receives an acknowledgment or the maximum number of explorer frame retries is reached.

You can use this command only after enabling DLSw v2.0 multicast.

Example # Set the maximum number of explorer frame transmission retries to 10.

```
<Sysname> system-view
[Sysname] dlsw max-transmission 10
```

dlsw multicast

Syntax **dlsw multicast** [*multicast-ip-address*] **interface** *interface-type interface-number*

undo dlsw multicast

View System view

Parameter *multicast-ip-address*: Multicast IP address, in the range of 224.0.10.0 to 224.0.10.191. The default is to 224.0.10.0.

interface: Specifies the interface through which DLSw v2.0 multicasts are sent.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **dlsw multicast** command to enable the multicast function of DLSw v2.0.

Use the **undo dlsw multicast** command to disable the multicast function of DLSw v2.0.

By default, the multicast function of DLSw v2.0 is disabled.

Related command: **dlsw enable**, **igmp enable** on page 1350, and **pim dm** on page 1411 and **pim sm** on page 1416.

Example # Enable the router to send DLSw 2.0 multicasts to the multicast address of 224.0.10.10 through Ethernet 1/0.

```
<Sysname> system-view
[Sysname] dlsw multicast 224.0.10.10 interface ethernet 1/0
```

dlsw timer

Syntax

dlsw timer { **cache** | **connected** | **explorer** | **explorer-wait** | **local-pending** | **remote-pending** } *seconds*

undo dlsw timer { **cache** | **connected** | **explorer** | **explorer-wait** | **local-pending** | **remote-pending** }

View

System view

Parameter

cache *seconds*: Timeout time of addresses in SNA cache, in seconds. The effective range is 1 to 65,535, and the default is 120 seconds.

connected *seconds*: Connection timeout time in seconds. The effective range is 1 to 65,535, and the default is 300 seconds.

explorer *seconds*: Remote explorer frame waiting time in seconds. The effective range is 1 to 65,535, and the default is 30 seconds.

explorer-wait *seconds*: Local explorer frame waiting time in seconds. The effective range is 1 to 65,535, and the default is 30 seconds.

local-pending *seconds*: Local pending time in seconds. The effective range is 1 to 65,535, and effective the default is 30 seconds.

remote-pending *seconds*: Remote pending time in seconds. The effective range is 1 to 65535, and the default is 30 seconds.

Description

Use the **dlsw timer** command to configure DLSw timers.

Use the **undo dlsw timer** command to restore DLSw timers to the default settings.

You can configure the timers used in creating DLSw circuits to meet your actual needs. Do this only when necessary.

Example

Configure DLSw timers as follows:

- Connection timeout time: 200 seconds
- local explorer frame waiting time: 15 seconds
- Local pending time: 15 seconds
- Remote pending time: 25 seconds
- SNA cache address timeout time: default
- Remote explorer frame waiting time: default

```
<Sysname> system-view
[Sysname] dlsw timer connected 200
[Sysname] dlsw timer explorer-wait 15
[Sysname] dlsw timer local-pending 15
[Sysname] dlsw timer remote-pending 25
```

idle-mark

Syntax **idle-mark**

undo idle-mark

View Synchronous serial interface view

Parameter None

Description Use the **idle-mark** command to configure the idle-time encoding scheme of the synchronous serial interface to be 0xFF.

Use the **undo idle-mark** command to restore the default setting.

By default, the synchronous serial interface uses "0x7E" to indicate its idle state.

While most SDLC devices use "0x7E" (flags) to indicate "idle" space between frames, some other SDLC devices use "0xFF" (marks) for this indication. For compatibility with different types of devices, you can configure the router to send either flags (default) or marks to indicate its idle state. When the synchronous serial interface is connected with an AS/400 device, you need to change the idle-time encoding scheme by using this command to improve the speed of polling the AS/400 device.

Example # Configure synchronous serial interface Serial 2/0 to send 0xFF to indicate idle space between frames.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] idle-mark
```

link-protocol sdlc

Syntax **link-protocol sdlc**

View Synchronous serial interface view

Parameter None

Description Use the **link-protocol sdlc** command to configure the synchronous serial interface to use SDLC as link layer encapsulation protocol.

By default, the default link layer protocol is PPP.

For SNA, SDLC is a link layer protocol, working very similarly as HDLC. To ensure that DLSw works normally, you need to enable SDLC as the link layer encapsulation protocol on the synchronous serial interface.

Note that you need to remove all IP related configurations on the interface before enabling SDLC, because SDLC cannot underlie the IP protocol. For example, you need to delete the IP address of the interface.

Example # Configure Serial 2/0 to use SDLC as the link layer encapsulation protocol.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol sdlc
```

llc2 max-ack

Syntax **llc2 max-ack** *length*

undo llc2 max-ack

View Ethernet interface view

Parameter *length*: The maximum number of information frames the router can receive before it must send an acknowledgment, in the range of 1 to 127.

Description Use the **llc2 max-ack** command to configure namely the maximum number of information frames the device can receive before it must send an acknowledgment to the peer router.

Use the **undo llc2 max-ack** command to restore the default setting.

By default, the maximum number of information frames the router can receive before it must send an acknowledgment is 3.

Example # Set the maximum number of information frames the router can receive before it must send an acknowledgment to 5 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 max-ack 5
```

llc2 max-pdu

Syntax **llc2 max-pdu** *length*

undo llc2 max-pdu

View Ethernet interface view

Parameter *length*: Maximum LLC2 PDU size in bytes, in the range of 1 to 1,700.

Description Use the **max-pdu** command to configure the maximum LLC2 PDU size.

Use the **undo max-pdu** command to restore the default maximum LLC2 PDU size.

By default, the maximum LLC2 PDU size is 1,493 bytes.

Example # Set the maximum LLC2 PDU size to 1,000 bytes on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 max-pdu 1000
```

llc2 max-send-queue

Syntax **llc2 max-send-queue** *length*

undo llc2 max-send-queue

View Ethernet interface view

Parameter *length*: The length of the LLC2 output queue, in the range of 20 to 200.

Description Use the **llc2 max-send-queue** command to configure the length of the LLC2 output queue.

Use the **undo llc2 max-send-queue** command to restore the default setting.

By default, the length of the LLC2 output queue is 50.

Example # Set the length of the LLC2 output queue to 30 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 max-send-queue 30
```

llc2 max-transmission

Syntax **llc2 max-transmission** *retries*

undo llc2 max-transmission

View Ethernet interface view

Parameter *retries*: LLC2 transmission retries, in the range of 1 to 255.

Description Use the **llc2 max-transmission** command to configure the number of LLC2 transmission retries, namely the maximum number of times an information frame is retransmitted before an acknowledgment frame is received from the peer.

Use the **undo llc2 max-transmission** command to restore the default setting.

By default, the number of LLC2 transmission retries is 3.

Example # Set the number of LLC2 transmission retries to 10 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 max-transmission 10
```

llc2 modulo

Syntax **llc2 modulo** { **8** | **128** }

undo llc2 modulo

View Ethernet interface view

Parameter **8**: Specifies the modulus value to be 8.

128: Specifies the modulus value to be 128.

Description Use the **llc2 modulo** command to configure the modulus of LLC2.

Use the **undo llc2 modulo** command to restore the default modulus of LLC2.

By default, the modulus of LLC2 is 128.

LLC2, like X.25, uses modulus to number frames. All frames sent are numbered incrementally and await an acknowledgment. When the frame number reaches the configured value (referred to as "modulus value"), subsequent frames are numbered from 1 again. For example, if the modulus value is set to 8, frames are numbered ...4, 5, 6, 7, 0, 1, ...

LLC2 supports two modulus values: 8 or 128. 128 is usually used for Ethernet frames.

Example # Set the modulus value for LLC2 frames to 8 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 modulo 8
```

llc2 receive-window

Syntax **llc2 receive-window** *length*

undo llc2 receive-window

View Ethernet interface view

Parameter *length*: The maximum number of consecutive information frames the router can send before receiving an acknowledgment from the peer, in the range of 1 to 127.

Description Use the **llc2 receive-window** command to configure the maximum number of consecutive information frames the router can send before receiving an acknowledgment from the peer.

Use the **undo llc2 receive-window** command to restore the default setting.

By default, the maximum number of consecutive information frames the router can send before receiving an acknowledgment from the peer is 7.

Example # Set the maximum number of consecutive information frames the router can send before receiving an acknowledgment from the peer to 10 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 receive-window 10
```

llc2 timer ack

Syntax **llc2 timer ack** *mseconds*

undo llc2 timer ack

View Ethernet interface view

Parameter *mseconds*: LLC2 acknowledgment waiting time in milliseconds. The effective range is 1 to 60,000.

Description Use the **llc2 timer ack** command to configure the LLC2 acknowledgment waiting time, namely the maximum length of time the router waits for an acknowledgment from the peer after sending an LLC2 frame.

Use the **undo llc2 timer ack** command to restore the default setting.

By default, the LLC2 acknowledgment waiting time is 200 milliseconds.

Example # Set the LLC2 acknowledgment waiting time to 10 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer ack 10
```

llc2 timer ack-delay

Syntax **llc2 timer ack-delay** *mseconds*

undo llc2 timer ack-delay

View Ethernet interface view

Parameter *mseconds*: LLC2 local acknowledgment delay, in milliseconds. The effective range is 1 to 60,000.

Description Use the **llc2 timer ack-delay** command to configure the LLC2 local acknowledgment delay time, namely the maximum length of time the device waits before sending an acknowledgment to the peer end upon receiving an LLC2 frame.

Use the **undo llc2 timer ack-delay** command to restore the default setting.

By default, the LLC2 local acknowledgment delay time is 100 milliseconds.

Example # Set the LLC2 local acknowledgment delay time to 200 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer ack-delay 200
```

llc2 timer busy

Syntax **llc2 timer busy** *mseconds*

undo llc2 timer busy

View Ethernet interface view

Parameter *mseconds*: LLC2 busy-station polling interval, in milliseconds. The effective range is 1 to 60,000. The system default is 300 milliseconds.

Description Use the **llc2 timer busy** command to configure the LLC2 busy-station polling interval, namely the amount of time the router waits before repelling a busy station.

Use the **undo llc2 timer busy** command to restore the default setting.

Example # Set the LLC2 busy-station polling interval to 200 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer busy 200
```

llc2 timer detect

Syntax **llc2 timer detect** *mseconds*

undo llc2 timer detect

View Ethernet interface view

Parameter *mseconds*: LLC2 POLL timer length in milliseconds. The effective range is 1 to 60,000.

Description Use the **llc2 timer detect** command to configure the LLC2 POLL timer, namely the interval at which both ends of a virtual circuit sends/receives Receiver Ready (RR) frames after the virtual circuit is established.

Use the **undo llc2 timer detect** command to restore the default setting.

By default, the LLC2 POLL timer length is 30,000 milliseconds.

Example # Set the LLC2 POLL timer length to 10,000 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer detect 10000
```

llc2 timer poll

Syntax **llc2 timer poll** *mseconds*

undo llc2 timer poll

View Ethernet interface view

Parameter *mseconds*: LLC2 P/F waiting time in milliseconds. The effective range is 1 to 60,000.

Description Use the **llc2 timer poll** command to configure the LLC2 P/F waiting time, namely the amount of time the router waits for an acknowledgment after sending a P frame.

Use the **undo llc2 timer poll** command to restore the default setting.

By default, the LLC2 P/F waiting time is 5,000 milliseconds.

When a router sends a frame that requires an acknowledgment, the frame is sent with a poll bit set. This frame is known as a P frame. Once the router sends a P frame, it cannot send any other P frame until it receives an acknowledgment, namely a frame with a final bit set, or until the LLC2 P/F waiting time expires.

Example # Set the LLC2 P/F waiting time to 2,000 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer poll 2000
```

llc2 timer reject

Syntax **llc2 timer reject** *mseconds*

undo llc2 timer reject

View Ethernet interface view

Parameter *mseconds*: LLC2 REJ status time in milliseconds. The effective range is 1 to 60,000.

Description Use the **llc2 timer reject** command to configure the LLC2 REJ status time, namely the amount of time the router waits for the expected frame after it receives an unexpected frame and sends a reject frame.

Use the **undo llc2 timer reject** command to restore the default setting.

By default, the LLC2 REJ status time is 500 milliseconds.

Example # Set the LLC2 REJ time to 2, 000 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] llc2 timer reject 2000
```

reset dlsw circuits

Syntax **reset dlsw circuits** [*circuit-id*]

View User view

Parameter *circuit-id*: DLSw virtual circuit ID, in the range of 0 to 0xFFFFFFFF.

Description Use the **reset dlsw circuits** command to clear DLSw virtual circuit information.

Note that this command without *circuit-id* clears the information of all DLSw virtual circuits; otherwise, this command clears the information of the specified virtual circuit.

Example # Clear the information of virtual circuit 100.

```
<Sysname> reset dlsw circuits 100
```

reset dlsw reachable-cache

Syntax **reset dlsw reachable-cache**

View User view

Parameter None

Description Use the **reset dlsw reachable-cache** command to clear DLSw reachability information.

Example # Clear the DLSw reachability information.

```
<Sysname> reset dlsw reachable-cache
```

reset dlsw tcp

Syntax **reset dlsw tcp** [*ip-address*]

View User view

Parameter *ip-address*: IP address of the remote peer.

Description Use the **reset dlsw tcp** command to reset the TCP connection between the DLSw router and a remote peer or all remote peers.

Note that:

- This command without *ip-address* resets the TCP connections between the DLSw router and all current remote peers; otherwise, this command resets the TCP connection between the DLSw router and the specified remote peer.
- In the case of a manual configured remote peer, this command disconnects the current TCP connection, and initiates a new TCP connection request to establish new TCP connection.
- In the case of a remote peer dynamically learned, this command disconnects the current TCP connection and deletes the remote peer.

Example # Reset the TCP connections will all remote peers.

```
<Sysname> debugging dlsw tcp
<Sysname> reset dlsw tcp
DLSw_TCP 4.4.4.2:The remote peer is learned dynamically ,it will be deleted
DLSW_TCP 4.4.4.3:Rebulid tcp with the peer
```

Reset the TCP connection with a remote peer with the IP address of 4.4.4.2.

```
<Sysname> reset dlsw tcp 4.4.4.2
DLSw_TCP 4.4.4.2:The remote peer is learned dynamically ,it will be deleted
```

Table 38 Description on the fields of the reset dlsw tcp command

Field	Description
DLSw_TCP 4.4.4.2:The remote peer is learned dynamically,it will be deleted	The remote peer 4.4.4.2 was learned dynamically and will be deleted by DLSw.
DLSW_TCP 4.4.4.3 : rebuild tcp with the peer	The remote peer 4.4.4.3 was manually configured and therefore the TCP connection with it will be reestablished.

Table 38 Description on the fields of the reset dlsw tcp command

Field	Description
Error: Wrong IP address	Invalid IP address entered
Error: No specified peer is found	The specified peer does not exist.

sdlc controller

Syntax **sdlc controller** *sdlc-address*

undo sdlc controller *sdlc-address*

View Synchronous serial interface view

Parameter *sdlc-address*: Address of the secondary SDLC station to be configured, in the range of 0x01 to 0xFE.

Description Use the **sdlc controller** command to configure the address of a secondary SDLC station address.

Use the **undo sdlc controller** command to delete the address of an secondary SDLC station.

By default, no secondary SDLC station address is configured.

The SDLC protocol allows multiple virtual circuits to run on an SDLC physical link, with one end connected to the primary station and the other end connected to the secondary station. In order to distinguish different virtual circuits, you need to specify an SDLC address for each virtual circuit.

SDLC is an "unbalanced" protocol: a primary station can be connected with multiple secondary devices through a multi-user system or an SDLC switch, while the secondary devices cannot be connected with one another. Therefore, the communication between the primary station and each secondary station can be guaranteed as long as each secondary device is identified with an SDLC address. This command is used to specify an SDLC address for a virtual circuit, which is unique on a physical interface.

The configured SDLC address on a synchronous serial interface is actually the address of a secondary SDLC station.

- On the serial interface of the DLSw router connected with the primary SDLC station, you need to configure the address of each secondary SDLC station that communicates with the primary station.
- On the serial interface of the DLSw router connected with a secondary SDLC station, you need to configure the address of each secondary SDLC station connected with the serial interface.

An SDLC address ranges from 0x01 to 0xFE. The SDLC address of a router is valid on only one physical interface. That is, the SDLC addresses configured on different interfaces may be the identical.

Example # Set the secondary SDLC station address to 0x05 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc controller 05
```

sdlc enable dlsw

Syntax **sdlc enable dlsw**

undo sdlc enable dlsw

View Synchronous serial interface view

Parameter None

Description Use the **sdlc enable dlsw** command to enable DLSw forwarding on the current synchronous serial interface.

Use the **undo sdlc enable dlsw** command to disable DLSw forwarding on the current synchronous serial interface.

By default, DLSw forwarding is not enabled on the serial interface.

Before enabling DLSw forwarding on the serial interface, enable SDLC as the link layer protocol on the interface. With DLSw forwarding enabled on the SDLC interface, all local SNA devices connected to the interface will be able to communicate with the remote device through DLSw.

Example # Enable DLSw forwarding on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol sdlc
[Sysname-Serial2/0] sdlc enable dlsw
```

sdlc mac-map local

Syntax **sdlc mac-map local** *mac-address*

undo sdlc mac-map local

View Synchronous serial interface view

Parameter *mac-address*: Virtual MAC address of SDLC.

Description Use the **sdlc mac-map local** command to configure an SDLC virtual MAC address.

Use the **undo sdlc mac-map local** command to delete the configured SDLC virtual MAC address.

By default, no SDLC virtual MAC address is configured.

Initially designed for LLC2 protocols, DLSw establishes mappings with virtual circuits through MAC addresses. Therefore, a MAC address must be specified for an SDLC virtual circuit so that SDLC frames can be forwarded. This command is used to assign the current interface a virtual MAC address, which will serve as the source MAC address during the conversion of SDLC frames to LLC2 frames.

Note that the sixth byte of the MAC address should be set to 0x00. The system will combine the first five bytes of this virtual MAC address with the SDLC address into a new MAC address, which will serve as the source MAC address in SDLC-to-LLC2 frame format conversion.

Example # Set the SDLC virtual MAC address to 0000-e81c-b600 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc mac-map local 0000-e81c-b600
```

sdlc mac-map remote

Syntax **sdlc mac-map remote** *mac-addr sdlc-addr*

undo sdlc mac-map remote *mac-addr sdlc-addr*

View Synchronous serial interface view

Parameter *mac-addr*: MAC address of the SDLC peer to be configured.

sdlc-addr: SDLC address of the SDLC peer to be configured, in the range of 0x01 to 0xFE.

Description Use the **sdlc mac-map remote** command to configure an SDLC peer.

Use the **undo sdlc mac-map remote** command to delete an SDLC peer.

By default, the synchronous serial interface has no remote peer.

This command is used to specify the MAC address of the corresponding peer end for an SDLC virtual circuit so as to provide the destination MAC address for SDLC-to-LLC2 frame conversion. In DLSw configuration, a peer should be configured for each SDLC address. The MAC address of the peer should be the MAC address of the remote SNA device (physical address in the Ethernet or Token Ring format), or the compound MAC address obtained from SDLC virtual MAC address of the peer end and the SDLC address of the local end.

In this configuration, pay attention to the difference in bit order between token ring address and an Ethernet address:

- If the remote SDLC peer to be configured uses a token ring address, use its token ring address directly;
- If the remote SDLC peer uses an Ethernet address, reverse the bit order of the Ethernet address: for example, convert 00e0.fc03.a548 to 0007.3fc0.5a12. You are recommended to use the **dlsw reverse** command to avoid errors that may be introduced in manual conversion.

Example # Configure an SDLC peer on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc mac-map remote 00E0-FC00-0010 05
```

sdlc max-pdu

Syntax **sdlc max-pdu** *number*

undo sdlc max-pdu

View Synchronous serial interface view

Parameter *number*: Maximum SDLC PDU size in bytes, in the range of 1 to 17,600.

Description Use the **sdlc max-pdu** command to configure the maximum SDLC PDU size, namely the maximum size in bytes of a frame that the router can send, not including the frame check sequence (FCS), start flag and ending flag fields.

Use the **undo sdlc max-pdu** command to restore the default setting.

By default, the maximum SDLC PDU size is 265 bytes.

The maximum PDU size of some PU2.0 devices is 265 bytes, while that of an IBM AS/400 is 521 bytes. Typically, this maximum PDU size should be configured be the same as on the peer SDLC device.

Example # Set the maximum SDLC PDU size to 521 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc max-pdu 521
```

sdlc max-send-queue

Syntax **sdlc max-send-queue** *length*

undo sdlc max-send-queue

View Synchronous serial interface view

Parameter *length*: Length of the SDLC output queue, in the range of 20 to 255.

Description Use the **sdlc max-send-queue** command to configure the length of the SDLC output queue.

Use the **undo sdlc max-send-queue** command to restore the default setting.

By default, the length of the SDLC output queue is 50.

Example # Set the length of the SDLC output queue to 30 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc max-send-queue 30
```

sdlc max-transmission

Syntax **sdlc max-transmission** *retries*

undo sdlc max-transmission

View Synchronous serial interface view

Parameter *retries*: Maximum number of SDLC transmission retries, in the range of 1 to 255 times.

Description Use the **sdlc max-transmission** command to configure the maximum number of SDLC transmission retries, namely the number of times a frame is retransmitted before an acknowledgment is received from the peer.

Use the **undo sdlc max-transmission** command to restore the default setting.

By default, the maximum number of SDLC transmission retries is 20.

Example # Set the maximum SDLC transmission retries to 30 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc max-transmission 30
```

sdlc modulo

Syntax **sdlc modulo** { **8** | **128** }

undo sdlc modulo

View Synchronous serial interface view

Parameter **8**: Specifies the modulus value to be 8.

128: Specifies the modulus value to be 128.

Description Use the **sdlc modulo** command to configure the modulus of the SDLC.

Use the **undo sdlc modulo** command to restore the default setting.

By default, the SDLC modulus is 8.

Like X.25, SDLC uses the modulus method to number frames. All frames sent are numbered incrementally and await an acknowledgment. When the frame number reaches the configured value (referred to as "modulus value"), subsequent frames are numbered from 1 again. For example, if the modulus value is set to 8, frames are numbered ...4, 5, 6, 7, 0, 1, ...

SDLC normally uses 8 as the modulus value.

Example # Restore the modulus value of SDLC to the default setting on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] undo sdlc modulo
```

sdlc sap-map local

Syntax **sdlc sap-map local** *lsap sdlc-addr*

undo sdlc sap-map local *lsap sdlc-addr*

View Synchronous serial interface view

Parameter *lsap*: SAP address, in the range of 0x01 to 0xFE.

sdlc-addr: SDLC address, in the range of 0x01 to 0xFE.

Description Use the **sdlc sap-map local** command to configure the local SAP address to be used in SDLC-to-LLC2 frame format conversion.

Use the **undo sdlc sap-map local** command to restore the system default.

By default, the local SAP address used in SDLC-to-LLC2 frame format conversion is 0x04.

When an SDLC frame is converted into an LLC2 frame, a SAP address is needed in addition to the MAC address.

Generally speaking, the SAP address used by the SNA protocol is 0x04, 0x08 or 0x0C.

Related command: **sdlc sap-map remote**.

Example # Configure the SAP address to be used in SDLC-to-LLC2 frame format conversion on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc sap-map local 08 05
```

sdlc sap-map remote

Syntax **sdlc sap-map remote** *dsap sdlc-addr*

undo sdlc sap-map remote *dsap sdlc-addr*

View Synchronous serial interface view

Parameter *dsap*: SAP address of the DLSw peer device, in the range of 0x01 to 0xFE.

sdlc-addr: SDLC address, in the range of 0x01 to 0xFE.

Description Use the **sdlc sap-map remote** command to configure the SAP address of the remote DLSw device for use in SDLC-to-LLC2 frame format conversion.

Use the **undo sdlc sap-map remote** command to restore the system default.

By default, the SAP address of the remote DLSw device used in SDLC-to-LLC2 frame format conversion is 0x04.

When an SDLC frame is converted to an LLC2 frame, a SAP address is needed in addition to the MAC address.

Generally speaking, the SAP address used by the SNA protocol is 0x04, 0x08 or 0x0C.

Related command: **sdlc sap-map local**.

Example # Configure the SAP address of the remote DLSw device for use in SDLC-to-LLC2 frame format conversion on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc sap-map remote 0C 05
```

sdlc simultaneous

Syntax **sdlc simultaneous**

undo sdlc simultaneous

View Synchronous serial interface view

Parameter None

Description Use the **sdlc simultaneous** command to configure the SDLC synchronous serial interface to work in two-way simultaneous mode, so that the primary SDLC station can send data to and receive data from a secondary station at the same time.

Use the **undo sdlc simultaneous** command to restore the default mode.

By default, the data transmission mode is "alternate".

Example # Enable the two-way simultaneous mode for SDLC data on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc simultaneous
```

sdlc status

Syntax **sdlc status** { **primary** | **secondary** }

undo sdlc status { **primary** | **secondary** }

View Synchronous serial interface view

Parameter **primary**: Specifies that the SDLC device connected to the router is "secondary".

secondary: Specifies that the SDLC device connected to the router is "primary".

Description Use the **sdlc role** command to configure a SDLC role.

Use the **undo sdlc role** command to remove the configured SDLC role.

By default, the device has no role.

SDLC is an "unbalanced" link layer protocol. That is, the end systems across a TCP connection are not equal in the positions: one is primary and the other is secondary. The primary station, whose role is **primary**, plays a dominant role and controls the whole connection process. The secondary station, whose role is **secondary**, is controlled by the primary station. Therefore, we need to configure a role for an SDLC interface.

In the SDLC role configuration, the role of an interface should be determined by the role of the SDLC device to which this router is connected:

- If the SDLC device connected with the local router has a role of **primary**, the local interface should be configured to have a role of **secondary**;
- If the SDLC device connected with the local router has a role of **secondary**, the local interface should be configured to have a role of **primary**.

Generally, an IBM mainframe has a role of **primary**, while a terminal device such as a UNIX host or an Auto Teller Machine (ATM) has a role of **secondary**.

Example # Set the role of the SDLC device connected with Serial 2/0 to **primary**, and the role of the local interface to **secondary**.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc status secondary
```

sdlc timer ack

Syntax **sdlc timer ack** *mseconds*

undo sdlc timer ack

View Synchronous serial interface view

Parameter *mseconds*: Primary-station acknowledgment waiting time: in milliseconds. The effective range is 1 to 60,000.

Description Use the **sdlc timer ack** command to configure the primary-station acknowledgment waiting time, namely the amount of time the primary SDLC station waits for an acknowledgment from the receiving secondary station after sending an information frame.

Use the **undo sdlc timer ack** command to restore the default setting.

By default, the primary-station acknowledgment waiting time is 3,000 milliseconds.

Example # Set the primary-station acknowledgment waiting time to 2,000 milliseconds on Serial 2/0.

```
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc timer ack 2000
```

sdlc timer lifetime

Syntax **sdlc timer lifetime** *mseconds*

undo sdlc timer lifetime

View Synchronous serial interface view

Parameter *mseconds*: Secondary-station acknowledgment waiting time in milliseconds. The effective range is 1 to 60,000.

Description Use the **sdlc timer lifetime** command to configure the secondary-station acknowledgment waiting time, namely the amount of time a secondary SDLC station waits for an acknowledgment from the primary station after sending an information frame.

Use the **undo sdlc timer lifetime** command to restore the default setting.

By default, the secondary-station acknowledgment waiting time is 500 milliseconds.

Example # Set the secondary-station acknowledgment waiting time to 1,000 milliseconds on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc timer lifetime 1000
```

sdlc timer poll

Syntax **sdlc timer poll** *mseconds*

undo sdlc timer poll

View Synchronous serial interface view

Parameter *mseconds*: SDLC polling interval in milliseconds. The effective range is 1 to 10,000.

Description Use the **sdlc timer poll** command to configure the SDLC polling interval, namely the amount of time the primary station waits between polling two secondary stations.

Use the **undo sdlc timer poll** command to restore the default setting.

By default, SDLC polling interval is 1,000 milliseconds.

Example # Set the SDLC polling interval to 200 milliseconds on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc timer poll 200
```

sdlc window

Syntax **sdlc window** *length*

undo sdlc window

View Synchronous serial interface view

Parameter *length*: The maximum number of consecutive frames the device can send before receiving an acknowledgement from the peer, in the range of 1 to 7.

Description Use the **sdlc window** command to configure the maximum number of consecutive frames the device can send before receiving an acknowledgement from the peer.

Use the **undo sdlc window** command to restore the default setting.

By default, the maximum number of consecutive frames the device can send before receiving an acknowledgement from the peer is 7.

Example # Set the maximum number of consecutive frames the device can send before receiving an acknowledgement from the peer to 5 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc window 5
```

sdlc xid

Syntax **sdlc xid** *sdlc-address xid-number*

undo sdlc xid *sdlc-address*

View Synchronous serial interface view

Parameter *sdlc-address*: SDLC address corresponding to the XID to be configured, in the range of 0x01 to 0xFE. This address should be configured beforehand.

xid-number: XID of the SDLC-enabled device, a 4-byte integer, in the range of 1 to 0xFFFFFFFF. The first 12 bits indicate the network address, and the last 20 bits indicate the node number.

Description Use the **sdlc xid** command to configure the XID of the SDLC.

Use the **undo sdlc xid** command to delete the XID of the SDLC.

By default, no SDLC XID is configured on a synchronous serial interface.

An XID identifies a device in an SNA system. When configuring an SDLC connection, pay attention to the types of the connected SNA devices. Generally, there are two types of devices in an SNA system: PU2.0 and PU2.1. An XID has been configured on PU2.1 devices, so they can announce their identity by exchanging the XID. A PU2.0 device does not come with an XID. Therefore, this command is not needed on PU2.1 devices, but it is required on PU2.0 devices to specify an XID.

Example # Set the XID of the device whose SDLC address is 0x05 to 0x2000 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] sdlc xid 05 2000
```

22 FRAME RELAY CONFIGURATION COMMANDS

annexg

Syntax **annexg** {dce | **dte**}

undo annexg {dce | **dte**}

View DLCI interface view

Parameter **dce**: Specifies the DLCI interface as an Annex G DTE interface.

dte: Specifies the DLCI interface as an Annex G DCE interface.

Description Use the **annexg** command to configure the operating mode (Annex G DCE or Annex DTE) for a DLCI interface.

Use the **undo annexg** command to remove the configuration.

By default, a DLCI interface does operate in the Annex G DCE mode.

ANSI T1.617 Annex G defines the way to transmit X.25 packets using FR virtual circuits. Similar to normal X.25 interface, an Annex G interface transmits/receives X.25 PVC and X.25 SVC packets and can operate as an X.25 switching interface. You can set LAPB-/X.25-related parameters for a virtual circuit by applying an X.25 template to it.

Example # Create an Annex G DTE interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 100
[Sysname-fr-dlci-Serial2/0-100] annexg dte
```

display fr compress

Syntax **display fr compress** [interface *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display fr compress** command to display the statistics information about frame relay compression. If no interface is specified, the DLCI statistics information for all interfaces is displayed.

Related commands: **fr compression frf9**.

Example # Display the frame relay compression statistics information of FRF.9 stac.

```
<Sysname> display fr compress
Serial2/0
 -DLCI:22
    enable frame-relay compression
    uncompressed bytes send/receive : 0/0
    compressed bytes send/receive : 0/0
    1 min  avg ratio send/receive :  0.000/0.000
5 min  avg ratio send/receive :  0.000/0.000
```

Table 39 Description on the fields of the display fr compress command

Field	Description
enable frame-relay compression	Frame relay compression is enabled
uncompressed bytes send/receive	Size of the uncompressed data transmitted /received (in bytes)
compressed bytes send/receive	Size of the compressed data transmitted/received (in bytes)
1 min avg ratio send/receive	Average transmission/receiving rate during the latest one minute
5 min avg ratio send/receive	Average transmission/receiving rate during the latest five minutes

display fr dlci-switch

Syntax **display fr dlci-switch** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display fr dlci-switch** command to display the information about the configured FR switching to check if the frame relay switching of a user is correctly configured.

The interface specified by *interface-type interface-number* can only be a main interface. If no interface is specified, this command displays the information about all the main interfaces.

Example # Display the information of the configured FR switching.

```
<Sysname> display fr dlci-switch
Frame relay switch statistics
Status   Interface(Dlci)   <---------->   Interface(Dlci)
Inactive Serial2/1(100)                 Serial2/0(300)
```

Table 40 Description on the fields of the display fr dlci-switch command

Field	Description
Frame relay switch statistics	The statistics of frame relay switch
Status	The status of frame relay switching function
Interface(Dlci) <----------> Interface(Dlci)	Input interface and its DLCI, output interface and its DLCI.

display fr inarp-info

Syntax **display fr inarp-info** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number. It can only be a main interface.

Description Use the **display fr inarp-info** command to display statistics about frame relay inverse ARP (INARP) packets, including requests and replies, for the specified or all interfaces.

You may use this command to diagnose whether INARP is operating normally.

Related command: **fr inarp**.

Example # Display statistics about frame relay INARP packets.

```
<Sysname> display fr inarp-info
Frame relay InverseARP   statistics for interface Serial2/0 (DTE)
In ARP request    Out ARP reply    Out ARP request    In ARP reply
0                 0                1                  1
```

Table 41 Description on the fields of the display fr inarp-info command

Field	Description
Frame relay InverseARP statistics for interface Serial2/0 (DTE)	Display frame relay INARP packet statistics of the interface
In ARP request	Received ARP requests
Out ARP reply	Transmitted ARP replies
Out ARP request	Transmitted ARP requests
In ARP reply	Received ARP replies

display fr interface

Syntax **display fr interface** [*interface-type* { *interface-number* | *interface-number.subnumber* }]

View Any view

Parameter *interface-type* { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. The *interface-number* argument is a main interface number. The *subnumber* argument is a subinterface number, in the range 0 to 1023.

Description Use the **display fr interface** command to display information about the specified or all frame relay interfaces.

You can specify a main interface or a subinterface by providing the *interface-type* { *interface-number* | *interface-number.subnumber* } argument combination.

Example # Display information about all frame relay interfaces.

```
<Sysname> display fr interface
Serial2/0, multi-point, protocol up
Serial2/0.1, point-to-point, protocol down
```

Table 42 Description on the fields of the display fr interface command

Field	Description
Serial2/0, multi-point, protocol up	Frame relay interface, its type and link layer state
Serial2/0.1, point-to-point, protocol down	Subinterface, its type and link layer state

display fr lmi-info

Syntax **display fr lmi-info** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display fr lmi-info** command to display the statistics of LMI protocol frame.

The LMI protocol maintains current frame relay link by sending status enquiry packets and status packets. The displayed information helps you diagnose faults.

Example # Display the statistics about LMI protocol frames.

```
<Sysname> display fr lmi-info
Frame relay LMI statistics for interface Serial2/1 (DTE, Q933)
T391DTE = 10 (hold timer 10)
N391DTE = 6, N392DTE = 3, N393DTE = 4
out status enquiry = 96, in status = 85
status timeout = 3, discarded messages = 3
Frame relay LMI statistics for interface Serial2/0 (DCE, Q933)
T392DCE = 15, N392DCE = 3, N393DCE = 4
in status enquiry = 0, out status = 0
status enquiry timeout = 0, discarded messages = 0
```

Table 43 Description on the fields of the display fr lmi-info command

Field	Description
Frame relay LMI statistics for interface Serial2/1 (DTE, Q933)	Terminal type and LMI protocol type for the frame relay interface
T391DTE = 10 (hold timer 10)	DTE-side T.391 setting
N391DTE = 6, N392DTE = 3, N393DTE = 4	DTE-side N.391, N.392, and N.393 settings
out status enquiry = 96, in status = 85	Number of the state enquiry packets sent out through the interface and that of the state enquiry packets received through the interface
status timeout = 3, discarded messages = 3	Number of the state packets that are timed out and that of the discarded packets
Frame relay LMI statistics for interface Serial2/0 (DCE, Q933)	Serial2/0 (a frame relay interface) is a DCE interface conformed with the standard described in Q.933 appendix A
T392DCE = 15, N392DCE = 3, N393DCE = 4	The T392, N392, and N393 parameters of the DCE interface
in status enquiry = 0, out status = 0	Number of the status packets received through the interface and that of the status packets sent out through the interface
status enquiry timeout = 0, discarded messages = 0	Number of the state packets that are timed out and that of the discarded packets

display fr iphc

Syntax **display fr iphc** [**interface** interface-type interface-number]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number. It can only be a main interface.

Description Use the **display fr iphc** command to display statistics about frame relay FRF.20 compression for the specified or all interfaces.

Related command: **fr compression iphc**.

Example # Display statistics about frame relay FRF.20 (FRF.20 IPHC) compression.

```
<Sysname> display fr iphc
Serial2/0 -DLCI:100
  RTP header compression information:
    Compression:
        Total packets:              0 , Packets compressed:              0
        Link searches:              0 , Search missed     :              0
        Bytes saved  :              0 , Bytes sent        :              0
    Decompression:
        Total packets:              0 , Packets compressed:              0
        Errors       :             0
    Compression-connections: 16 , Decompression-connections: 16

  Information of TCP header compression:
    Compression:
```

```
    Total packets:              8 , Packets compressed:              5
    Link searches:              0 , Search Missed     :              1
    Bytes saved  :            173 , Bytes sent        :            598
Decompression:
    Total packets:              6 , Packets compressed:              4
    Errors       :              0
Compression-connections: 16 , Decompression-connections: 16
```

Table 44 Description on the fields of the display fr iphc command

Field	Description
RTP header compression information	Information of RTP header compression
Information of TCP header compression	Information of TCP header compression
Compression	Information of compression
Decompression	Information of decompression
Compression-connections	Number of most compression-connection
Total packets	Total number of packets
Packets compressed	Number of packets compressed
Link searches	Times of link search
Search missed	Times of search missed
Bytes saved	Number of bytes saved
Bytes sent	Number of bytes sent
Errors	Number of error
Compression-connections: 16 Decompression-connections: 16	The most connection number of compression and depression

display fr map-info

Syntax **display fr map-info** [**interface** *interface-type* { *interface-number* | *interface-number.subnumber* }]

View Any view

Parameter **interface** *interface-type* { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. It can be a main or subinterface. The *interface-type* argument is an interface type. The *interface-number* argument is a main interface number. The *subnumber* argument is a subinterface number, in the range 0 to 1023.

Description Use the **display fr map-info** command to display all frame relay address mappings or the one for the specified interface.

This command displays whether the static address map entries are correct and whether dynamic address mapping operates normally.

Related command: **fr map ip**, **fr inarp**.

Example # Display the frame relay address map table.

```
<Sysname> display fr map-info
Map Statistics for interface Serial2/0 (DTE)
DLCI = 100, IP INARP 100.100.1.1, Serial2/0
create time = 2002/10/21 14:48:44, status = ACTIVE
encapsulation = ietf, vlink = 14, broadcast
DLCI = 200, IP INARP 100.100.1.1, Serial2/0
create time = 2002/10/21 14:34:42, status = ACTIVE
encapsulation = ietf, vlink = 0, broadcast
DLCI = 300, IP 1.1.1.1, Serial2/0
create time = 2002/10/21 15:03:35, status = ACTIVE
encapsulation = ietf, vlink = 15
```

Table 45 Description on the fields of the display fr map-info command

Field	Description
Map Statistics for interface Serial2/0 (DTE)	Display the frame relay address map. The interface operates in DTE mode.
DLCI = 100, IP INARP 100.100.1.1, Serial2/0	The PVC with DLCI 100 is mapped to remote IP address 100.100.1.1 through INARP. The PVC is configured on the interface Serial2/0 (If the keyword INAPP is not provided, you need to manually configure established address mapping.)
create time = 2002/10/21 14:48:44	Time and date when the map entry was created
status = ACTIVE	State of the map entry
encapsulation = ietf	Encapsulation is set to IETF
broadcast	Broadcasts are permitted

display fr map-info pppofr

Syntax **display fr map-info pppofr** [**interface** *interface-type* { *interface-number* | *interface-number.subnumber* }]

View Any view

Parameter **interface** *interface-type* { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. It can be a main or subinterface. The *interface-type* argument is an interface type. The *interface-number* argument is a main interface number. The *subnumber* argument is a subinterface number, in the range 0 to 1023.

Description Use the **display fr map-info pppofr** command to display current PPP over frame relay (PPPoFR) mappings and their states for the specified or all interfaces.

Example # Display information about current PPPoFR mappings and their states.

```
<Sysname> display fr map-info pppofr
Fr Interface    DLCI    Fr State      PPP Interface         PPP Phase
Serial2/0     100     down          Virtual-Template1     Phase:0
Serial2/1     200     down          Virtual-Template2     Phase:0
```

Table 46 Description on the fields of the display fr map-info pppofr command

Field	Description
Fr Interface	Frame relay interface name
DLCI	DLCI number
Fr State	Frame relay state
PPP Interface	Name of the associated PPP virtual template interface
PPP Phase	Phase of the PPP session

display fr pvc-info

Syntax **display fr pvc-info** [**interface** *interface-type* { *interface-number* | *interface-number.subnumber* }] [*dlci-number*]

View Any view

Parameter **interface** *interface-type* { *interface-number* | *interface-number.subnumber* }: Specifies an interface by its type and number. It can be a main or subinterface. The *interface-type* argument is an interface type. The *interface-number* argument is a main interface number. The *subnumber* argument is a subinterface number, in the range 0 to 1023.

dlci-number: virtual circuit number of frame relay interface. It ranges from 16 to 1007.

Description Use the **display fr pvc-info** command to display state information on FR PVCs and statistics about data transmitted and received on them.

If the command is performed with no interface or DLCI specified, the displayed information covers all PVCs; if with an interface (a main interface or subinterface) specified, the displayed information covers only the PVCs on the interface; and if with a DLCI specified, the displayed information covers only the specified PVC.

Related command: **fr dlci**.

Example # Display the frame relay PVC table.

```
<Sysname> display fr pvc-info
PVC statistics for interface Serial2/0 (DTE, physical UP)
DLCI = 100, USAGE = UNUSED (0000), Serial2/0
create time = 2000/04/01 23:55:39, status = active
in BECN = 0, in FECN = 0
in packets = 0, in bytes = 0
out packets = 0, out bytes = 0
DLCI = 102, USAGE = LOCAL (0010), INTERFACE = Serial2/0.1
create time = 2000/04/01 23:56:14, status = active
in BECN = 0, in FECN = 0
in packets = 0, in bytes = 0
out packets = 0, out bytes = 0
```

Table 47 Description on the fields of the display fr pvc-info command

Field	Description
PVC statistics for interface Serial2/0 (DTE, physical UP)	Display information about PVCs on the frame relay interface Serial 2/0. The interface operates in as a DTE. The physical state of the interface is up.
DLCI = 100, USAGE = UNUSED (0000), INTERFACE = Serial2/0	DLCI 100 was assigned to the PVC through negotiation of LMI with DCE end. Its state is unused, and it belongs to interface Serial 2/0.
create time = 2000/04/01 23:55:39, status = active	Date and time creating the PVC and the state of the PVC
in BECN = 0, in FECN = 0	Received BECNs and FECNs
in packets = 0, in bytes = 0	Received frames and bytes
out packets = 0, out bytes = 0	Transmitted frames and bytes

display fr statistics

Syntax **display fr statistics** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number. This interface must be a main interface.

Description Use the **display fr statistics** command to display current frame relay statistics about received and transmitted packets for the specified or all interfaces.

You may use this command to check frame relay traffic statistics and diagnose problems.

Example # Display frame relay statistics about received and transmitted packets.

```
<Sysname> display fr statistics
Frame relay packet statistics for interface Serial2/0 (DTE)
in packets = 84, in bytes = 1333
out packets = 92, out bytes = 1217
discarded in packets = 13, discarded out packets = 0
Frame relay packet statistics for interface Serial2/0.1 (DCE)
in packets = 0, in bytes = 0
out packets = 0, out bytes = 0
discarded in packets = 0, discarded out packets = 0
```

Table 48 Description on the fields of the display fr statistics command

Field	Description
Frame relay packet statistics for interface Serial2/0 (DTE)	Display frame relay packet statistics for the interface Serial 2/0, which operates as a DTE.
in packets = 84, in bytes = 1333	Received packets and bytes
out packets = 92, out bytes = 1217	Transmitted packets and bytes
discarded in packets = 13, discarded out packets = 0	Dropped incoming/outgoing packets

display interface mfr

Syntax **display interface mfr** [*interface-number* | *interface-number.subnumber*]

View Any view

Parameter *interface-number*: MFR interface number, in the range 0 to 1023.

interface-number.subnumber: MFR subinterface number, of which, *interface-number* is the main interface number, and *subnumber* is subinterface number. The *subnumber* argument ranges from 0 to 1023.

Description Use the **display interface mfr** command to display the information about an MFR interface or an MFR sub-interface, including configuration, state, and packet statistics.

If you do not specify an MFR interface or an MFR sub-interface, this command displays the information about all the MFR interfaces.

Example # Display the configuration and status information about interface MFR4.

```
<Sysname> display interface mfr 4
MFR4 current state : UP
Line protocol current state : UP
Description : MFR4 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet Address is 12.12.12.2/16 Primary
Link layer protocol is FR IETF
  LMI DLCI is 0, LMI type is Q.933a, frame relay DTE
  LMI status enquiry sent 435, LMI status received 435
  LMI status timeout 0, LMI message discarded 0
Physical is MFR, baudrate: 2048000 bps
Output queue: (Urgent queue: Size/Length/Discards) 0/50/0
Output queue: (Protocol queue: Size/Length/Discards) 0/500/0
Output queue: (FIFO queuing: Size/Length/Discards) 0/75/0
Last 300 seconds input:  0 bytes/sec, 0 packets/sec
Last 300 seconds output:  0 bytes/sec, 0 packets/sec
     1058 packets input, 832389 bytes, 0 drops
     619 packets output, 828190 bytes, 0 drops
```

Table 49 Description on the fields of the display interface mfr command

Field	Description
MFR4 current state : UP	Physical layer state
Line protocol current state : UP	Link layer state
Description : MFR4 Interface	Interface description
The Maximum Transmit Unit is 1500	MTU
Internet Address is 12.12.12.2/16	IP address and mask
link-protocol is FR IETF	Link layer protocol
LMI DLCI is 0, LMI type is Q.933a, frame relay DTE	DLCI number used by LMI, LMI type, port type and operating mode

Table 49 Description on the fields of the display interface mfr command

Field	Description
LMI status enquiry sent 435, LMI status received 435	Transmitted and received LMI status enquiry messages
LMI status timeout 0, LMI message discarded 0	LMI timeout messages and dropped LMI messages
Physical is MFR	Physical interface is MFR
Output queue: (Urgent queue: Size/Length/Discards) 0/50/0	Statistics on the packets of the following interface output queues: ■ Urgent queue ■ Protocol queue ■ FIFO queue
Output queue: (Protocol queue: Size/Length/Discards) 0/500/0	
Output queue: (FIFO queuing: Size/Length/Discards) 0/75/0	
Last 300 seconds input: 0 bytes/sec, 0 packets/sec	Input rate of the interface within the last five minutes
Last 300 seconds output: 0 bytes/sec, 0 packets/sec	Output rate of the interface within the last five minutes
1058 packets input, 832389 bytes, 0 drops	Packets and bytes received on the interface and packets dropped as the result of full receive buffer
619 packets output, 828190 bytes, 0 drops	Packets and bytes transmitted on the interface and packets dropped as the result of full transmit buffer

display mfr

Syntax **display mfr** [**interface** *interface-type interface-number* | **verbose**]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

verbose: Displays detailed statistics information, including the number of controlling packets sent and received.

Description Use the **display mfr** command to display configuration and statistics information of multilink frame relay bundle and bundle link. If no bundle or bundle link is specified, information about all bundles and bundle links is displayed.

Example # Display configuration and state information about all frame relay bundles and frame relay bundle links.

```
<Sysname> display mfr
Bundle interface:MFR1, Bundle state = up,  Bundle class = A,
    fragment disabled, MFR bundle fragment size = 222
        original packet be assembled/fragmentized (in/out): 0/0
        dropped fragment (in/out): 0/0
    Bundle name = 2
    Bundle links:
    Serial2/0, PHY state = up, link state = up,  Link name : Serial2/0
```

Table 50 Description on the fields of the display mfr command

Field	Description
Bundle interface	Bundle interface
Bundle state	Operating state of the bundle interface.
Bundle class	Class A indicates if there is one bundle link is in up state, the bundle is flagged as up. Moreover, all bundle links should be tagged as down before the bundle is down.
fragment disabled	Indicates whether the fragment is disabled (disabled in this sample output)
MFR bundle fragment size	Maximum fragment size allowed by the FR link
Bundle name	Name of multilink frame relay bundle
Bundle links	Physical interfaces of the links in the bundle.
Serial2/0, PHY state = up, link state = up, Link name = Serial2/0	Physical interface on the bundle link, the operating state of the physical layer interface and link layer interface, the link name of the bundle link (corresponding name on the physical interface by default)

Display detailed state information about all frame relay bundle links.

```
<Sysname> display mfr verbose
Bundle interface:MFR1, Bundle state = up,  Bundle class = A,
    fragment enabled, MFR bundle fragment size = 222
        original packet be assembled/fragmentized (in/out): 0/0
        dropped fragment (in/out): 0/0
    Bundle name = 2
    Bundle links:
    LID : Serial2/0   Peer LID: Serial2/0
    Bound to MFR1(BID:2)
    Physical state: up, link state: up,
    Bundle link fragment size: 222,
    Bundle Link statistics:
        Hello(TX/RX):         10/10    Hello_ack(TX/RX):       10/10
        Add_link(TX/RX):      4/2    Add_link_ack(TX/RX):    2/1
        Add_link_rej(TX/RX):  0/0
        Remove_link(TX/RX):   0/0    Remove_link_ack(TX/RX):  0/0
        Pkts dropped(in/out): 0/0
        Timer: ACK  4, Hello  10
        Retry: Max  2, Current 0
        Cause code: none
    Bundle Link fragment statistics:
        Mfr fragment(in/out): 0/0
```

Table 51 Description on the fields of the display mfr verbose command

Field	Description
LID	Identifier of the bundle link (to be the name of corresponding physical interface by default)
Peer LID	Identifier of the peer bundle link (to be the name of corresponding physical interface by default).
Bound to MFR0 (BID:MFR0)	The bundle link is bound to MFR0 on the interface MFR
Physical state	Operating state of the physical interface.
link state	Operating state of the link protocol on the bundle link.
Bundle Link statistics:	Statistics about the packets on the bundle link.

Table 51 Description on the fields of the display mfr verbose command

Field	Description
Hello(TX/RX)	Number of the transmitted and received Hello messages. Hello messages are sent for maintaining link state.
Hello_ack(TX/RX)	Number of transmitted and received Hello acknowledgement messages. Hello_ack messages are sent notifying receipt of the Hello messages.
Add_link(TX/RX)	Number of transmitted and received Add_link messages. Add_link messages are sent notifying the peer that the local node is ready for processing frames.
Add_link_ack(TX/RX)	Number of transmitted and received Add_link acknowledgment messages. Add_link_ack messages are sent notifying receipt of the Add_link messages.
Add_link_rej(TX/RX)	Number of transmitted and received Add_link reject messages. Add_link_rej messages are sent notifying reject of the Add_link messages.
Remove_link(TX/RX)	Number of transmitted and received Remove_link messages. Remove_link messages are sent notifying removal of a link from the bundle.
Remove_link_ack(TX/RX)	Number of transmitted and received Remove_link_ack messages. Remove_link_ack messages are sent notifying receipt of the Remove_link messages.
Pkts dropped(in/out)	Number of dropped incoming and outgoing packets.
Timer: Ack 4	Time waiting for a Hello_ack message before a Hello message or an Add_link message (for initial synchronization) is retransmitted on the bundle link.
Hello 10	Intervals for sending Hello messages.
Retry: max 2	Maximum number of Hello or Add_link sending retries made when no Hello_ack or Add_link_ack is received on the bundle link.
Current 0	Number of retries
Cause code	Cause resulting in the current state of the bundle link.
Bundle Link fragment statistics	Fragment statistics on the bundle link

display x25 template

Syntax **display x25 template** [*name*]

View Any view

Parameter *Name*: Name of an X.25 template.

Description Use the **display x25 template** command to display the information of an X.25 template, including the configuration concerning X.25 and LAPB.

If you do not specify the *name* argument, this command displays the information of all the X.25 templates.

Related command: **x25 template**, **x25-template**.

Example # Display the configuration of the X.25 template named "vofr".

```
<Sysname> display x25 template vofr
  Template:vofr
    X25 parameters
      X121 address:none    Modulo:8
      Timers
        Idle:0 (second)  T10/T20:1  T11/T21:200  T12/T22:180  T13/T23:180
      Channels
        Incoming-only:disable  Two-way:1-1024  Outgoing-only:disable
      Window size
        In:2  Out:2
      Packet size
        In:128  Out:128
    LAPB parameters
      Modulo:8  K:7  N1:12056  N2:10
      Timers
        T1:3000  T2:1500  T3:0
```

Table 52 Description on t he fields of the display x25 template command

Field	Description
X25 parameters	X.25-related settings
X121 address	X.121 address
Modulo	Window modulo, which defaults to 8.
Timers	■ Idle: Maximum idle period of SVCs ■ T10/T20: Delay of the re-start/re-transmission timer ■ T11/T21: Delay of the call request transmission timer ■ T12/T22: Delay of the reset request transmission timer ■ T13/T23: Delay of the clear request transmission timer
Channels	■ Incoming-only: Channel range of incoming-only calls ■ Two-way: Two-way channel range ■ Outgoing-only: Channel range of outgoing-only calls
Window size	■ In: Receiving window size ■ Out: Transmitting window size
Packet size	■ In: Maximum X.25 packet size allowed for receiving ■ Out: Maximum X.25 packet size allowed for transmitting
LAPB parameters	LAPB-related settings
Modulo	Modulo for numbering LAPB frames
N1	Maximum packet size (in bytes) a DCE/DTE allows
N2	Maximum number of retries allowed for an DTE/DCE to transmit a packet
Timers	T1: Transmission timer T2: Receiving timer T3: Idle channel timer

fr compression frf9

Syntax **fr compression frf9**

undo fr compression

View Subinterface (point-to-point) view

Parameter None

Description Use the **fr compression frf9** command to enable FRF9 compression function.

Use the **undo fr compression** command to disable FRF9 compression function.

By default, frame relay compression function is disabled.

The system supports FRF.9 stac compression function, which groups messages into control messages and data messages. An control message is used for state negotiation between the two sides that have compression protocol enabled of a DLCI connection. FRF.9 data messages are exchanged only after the negotiation succeeds. The negotiation fails if the number of FRF.9 control messages sent exceeds. In this case, compression configuration cannot take effect.

Frame relay main interface is point-to-multipoint, but the subinterface includes two types: point-to-point and point-to-multipoint. Frame relay FRF.9 compression configuration differs depends on different types of interfaces. For a point-to-point frame relay subinterface, just use the **fr compression frf9** command to configure on the subinterface view and FRF.9 compression function is enabled. For a point-to-multipoint frame relay interface or subinterface, whether to perform FRF.9 compression is determined by the configuration to create static address mapping. Refer to "fr map ip" on page 396.

This command is only valid for data messages and IARP messages but not LMI messages.

Only when the frame relay packets type of the interface is IETF, can frame relay compression take effect. When this command is configured, the system will automatically change the packet type of the interface into IETF if the frame relay packets type of an interface is not IETF.

Example # Enable frame relay compression on the point-to-point frame relay subinterface Serial 2/1.1.

```
<Sysname> system-view
[Sysname] interface serial 2/1.1 p2p
[Sysname-Serial2/1.1] fr compression frf9
```

fr compression iphc

Syntax **fr compression iphc**

undo fr compression iphc

View Frame relay interface view

Parameter None

Description Use the **fr compression iphc** command to enable FRF.20 (FRF.20 IPHC) compression.

Use the **undo fr compression iphc** command to disable the function.

By default, the frame relay compression function is disabled.

The system supports frame relay FRF.20 IP Header Compression (IPHC) function that compresses IP header. This technology is used to transmit voice messages so as to save bandwidth, and data is transmitted with great efficiency and speed.

Messages are divided into control messages and data messages according to FRF.20. An control message is used for state negotiation between the two sides that have compression protocol enabled of a DLCI connection. FRF.20 data messages are exchanged only after the negotiation succeeds. The negotiation fails if the number of FRF.20 control messages sent exceeds. In this case, compression configuration cannot take effect. This command is only valid for RTP messages and TCP ACK messages.

You can specify FRF.20 (FRF.20 IPHC) compression function using either the **fr compression iphc** command or configuring static address mapping.

For detailed information about configuring static address mapping, refer to "fr map ip" on page 396.

Example # Configure the frame relay interface Serial 2/0 to adopt FRF.20 compression.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr compression iphc
```

fr dlci

Syntax **fr dlci** *dlci-number*

undo fr dlci [*dlci-number*]

View Interface view

Parameter *dlci-number*: Virtual circuit number allocated for the frame relay interface, in the range 16 to 1007. The range 0 to 15 and 1008 to 1023 are reserved for special purposes.

Description Use the **fr dlci** command to configure the virtual circuit for frame relay interface and enter the corresponding virtual circuit view on the frame relay.

Use the **undo fr dlci** command to cancel the configuration.

When the frame relay interface type is DCE or NNI, it is necessary to manually configure virtual circuit for interface (either main interface or subinterface). When the frame relay interface type is DTE, if the interface is main interface, the system will automatically configure the virtual circuit according to the peer device.

The virtual circuit number on the physical interface is unique.

Example # Assign a virtual circuit with DLCI 100 to frame relay interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 100
[Sysname-fr-dlci-Serial2/0-100]
```

fr dlci-switch

Syntax **fr dlci-switch** *in-dlci* **interface** *interface-type interface-number* **dlci** *out-dlci*

undo fr dlci-switch *in-dlci*

View Frame relay interface view, MFR interface view

Parameter *in-dlci*: DLCI in the packets received on the interface, in the range 16 to 1007.

interface *interface-type interface-number*: Specifies an interface by its type and number.

dlci *out-dlci*: DLCI in the sent packets. It is in the range 16 to 1007.

Description Use the **fr dlci-switch** command to configure a static route for frame relay PVC switching.

Use the **undo fr dlci-switch** command to delete a static route for frame relay PVC switching.

By default, no static route is configured for frame relay PVC switching.

Before the static route of frame relay PVC is configured, it is necessary to enable the frame relay PVC switching first by using the **fr switching** command.

The default type of the forwarding interface can be frame relay or MFR. You can however specify a tunnel interface for forwarding, if one has been configured, thus transmitting frame relay packets over IP networks.

Related command: **fr switching**.

Example # Configure a static route, allowing the packets on the link with DLCI of 100 on Serial 2/0 to be forwarded over the link with DLCI of 200 on interface Serial 2/1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci-switch 100 interface serial 2/1 dlci 200
```

Configure a static route, allowing the packets on the link with DLCI of 200 on Serial 2/1 to be forwarded over the link with DLCI of 300 on tunnel interface 4.

```
<Sysname> system-view
[Sysname] interface serial 2/1
[Sysname-Serial2/1] fr dlci-switch 200 interface tunnel 4 dlci 300
```

fr inarp

Syntax **fr inarp** [**ip** [*dlci-number*]]

undo fr inarp [**ip** [*dlci-number*]]

View Interface view

Parameter **ip**: Performs inverse address resolution for IP addresses.

dlci-number: Data link connection identifier number, that is, virtual circuit number, indicating that the inverse address resolution is performed for this DLCI number only, ranges from 16 to 1007.

Description Use the **fr inarp** command to enable the inverse address resolution of frame relay.

Use the **undo fr inarp** command to disable this function.

By default, system permits enabling the frame relay inverse address resolution.

When the frame relay sends data over the interface, it is necessary to map the network address to the DLCI numbers. Such a map can be specified manually or can be completed via the function of automatic inverse address resolution. Automatic inverse address resolution can be started by using the command.

If it is expected to enable the inverse address resolution function of all PVCs, the command without any parameters is adopted.

If it is expected to disable the inverse address resolution function of all PVCs, the command **undo** without any parameters is adopted.

If it is expected to enable the inverse address resolution function in the specified data link, the command with *dlci-number* parameter is adopted.

By default, inverse address resolution function is enabled on the interface, including the subinterface, so are the PVCs on the interface. In this case, use **undo fr inarp ip** *dlci-number* command to disable the address solution function on a virtual circuit. If you use **undo fr inarp** command to disable the address solution function on an interface, the function of all the virtual circuits on the interface is disabled but the **fr inarp ip** *dlci-number* command is used to enable address resolution function on a virtual circuit.

The **fr inarp** command configured on an FR main interface also applies to its subinterfaces.

Example # Enable InARP at all PVCs of the frame relay interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr inarp
```

fr interface-type

Syntax **fr interface-type { dce | dte | nni }**

undo fr interface-type

View Interface view

Parameter **dce**: Set the type of frame relay interface to DCE (Data Circuit-terminating Equipment).

dte: Set the type of frame relay interface to DTE (Data Terminal Equipment).

nni: Set the type of frame relay interface to NNI (Network-to-Network Interface).

Description Use the **fr interface-type** command to set the frame relay interface type.

Use the **undo fr interface-type** command to restore the default frame relay interface type.

By default, the frame relay interface type is DTE.

In frame relay, there are two communicating parties, namely, the user side and network side. The user side is called Data Terminal Equipment (DTE), and the network side is called Data Communications Equipment (DCE). In a frame relay network, the interface between the frame relay switches is Network-to-Network Interface (NNI), and the corresponding interface adopts the NNI operating view. If the device is used as frame relay switching, the frame relay interface should operate in the NNI view or DCE mode. The system supports the three modes.

While configuring the frame relay interface type as DCE or NNI, it is unnecessary to perform the **fr switching** command in the System view. Please note that this is different from the mainstream equipment in the communications field.

Example # Set the type of the frame relay interface Serial 2/0 to DCE.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] fr interface-type dce
```

fr iphc

Syntax **fr iphc** { **nonstandard** | **rtp-connections** *number1* | **tcp-connections** *number2* | **tcp-include** }

undo fr iphc { **nonstandard** | **rtp-connections** | **tcp-connections** | **tcp-include** }

View Frame relay interface view, MFR interface view

Parameter **nonstandard**: Nonstandard compatible compression format.

rtp-connections number1: The number of RTP compression connections, in the range 3 to 1000. By default, the number of RTP compression connections is 16.

tcp-connections number2: The number of TCP compression connections, in the range 3 to 256. By default, the number of TCP compression connections is 16.

tcp-include: Includes TCP header compression when performing RTP compression.

Description Use the **fr iphc** command to enable IP header compression function, including RTP/TCP header compression.

Use the **undo fr iphc** { **nonstandard | tcp-include** } command to disable this function.

Use the **undo fr iphc** { **rtp-connections | tcp-connections** } command to restore the default compression connection numbers of RTP and TCP.

By default, *number1* and *number2* are 16.

Related command: **fr map ip**, **fr compression iphc**.

Example # Configure the number of RTP compression connections as 200 on the frame relay Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] fr iphc rtp-connections 200
```

fr lmi n391dte

Syntax **fr lmi n391dte** *n391-value*

undo fr lmi n391dte

View Interface view

Parameter *n391-value*: The value of counter N391, ranges from 1 to 255.

Description Use the **fr lmi n391dte** command to configure N391 parameter at the DTE side.

Use the **undo fr lmi n391dte** command to restore the default.

By default, the parameter value is 6.

The DTE sends a Status-Enquiry packet at regular interval set by T391 to the DCE. There are two types of Status-Enquiry packets: link integrity authentication packet and link status enquiry packet. The N391 parameter defines the ratio of sending the two types of packets, that is, link integrity authentication packets: link status enquiry packets = (N391 - 1): 1.

Example # Set DTE as the operating mode of frame relay interface Serial 2/0, and the counter value of the PVC status to 10.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dte
[Sysname-Serial2/0] fr lmi n391dte 10
```

fr lmi n392dce

Syntax **fr lmi n392dce** *n392-value*

undo fr lmi n392dce

View Interface view

Parameter *n392-value*: The Error threshold, which ranges from 1 to 10.

Description Use the **fr lmi n392dce** command to set N392 parameter at the DCE side.

Use the **undo fr lmi n392dce** command to restore the default.

By default, the parameter value is 3.

The DCE requires the DTE to send a Status-Enquiry packet at regular interval (set by T392). If the DCE does not receive the Status-Enquiry packet within a period of time, the error counter on DCE increments by one. If the errors exceed the threshold, the DCE would consider the physical channels and all the DLCIs to be unavailable.

N392 and N393 together define the "error threshold". N393 defines the event number observed and N392 defines the error threshold of that number (N393). That is, if number of errors that occurred to the DCE reaches N392 in N393 events, DCE will consider the errors have reached the threshold and declare the physical channels and all DLCIs to be unavailable.

N392 should be less than N393.

Example # Set frame relay interface Serial 2/0 to operate in DCE mode and set N392 to 5 and N393 to 6.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr lmi n392dce 5
[Sysname-Serial2/0] fr lmi n393dce 6
```

fr lmi n392dte

Syntax **fr lmi n392dte** *n392-value*

undo fr lmi n392dte

View Interface view

Parameter *n392-value*: The value of N392 parameter at the DTE side. It ranges from 1 to 10.

Description Use the **fr lmi n392dte** command to set N392 parameter at the DTE side.

Use the **undo fr lmi n392dte** command to restore the default.

By default, the parameter value is 3.

The DTE sends a Status-Enquiry packet at a regular interval to the DCE to inquire the link status. On receiving this packet, the DCE will immediately send a Status-Response packet. If the DTE does not receive the response packet in the specified time, it will record the error by adding 1 to the error count. If the errors exceed the threshold, the DTE will consider that the physical channels and all the DLCIs to be unavailable.

N392 and N393 together define the "error threshold". N393 indicates the event number observed and N392 indicates the error threshold of that number (N393). That is, if N392 errors occurred in N393 Status-Enquiry packets in the DTE, the DTE would consider that the error had exceeded the threshold and declare the physical channels and all DLCIs to be unavailable.

N392 at DTE side should be less than N393 at DTE side.

Example # Set the operation of frame relay interface Serial 2/0 as the DTE mode and set N392 to 5 and N393 to 6.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr lmi n392dce 5
[Sysname-Serial2/0] fr lmi n393dce 6
```

fr lmi n393dce

Syntax **fr lmi n393dce** *n393-value*

undo fr lmi n393dce

View Interface view

Parameter *n393-value*: The value of N392 parameter at the DTE side. It ranges from 1 to 10.

Description Use the **fr lmi n393dce** command to set the N393 parameter at the DCE side.

Use the **undo fr lmi n393dce** command to restore the default.

By default, the parameter value is 4.

The DCE requires the DTE to send a Status-Enquiry packet at a regular interval (set by T392). If the DCE does not receive the Status-Enquiry packet, it will record the error by adding 1 to the error count. If the errors exceed the threshold, the DCE would consider the physical channels and all the DLCIs to be unavailable.

N392 and N393 together define the "error threshold". N393 defines the event number observed and N392 defines the error threshold of that number (N393). That is, if the number of errors that occur to the DCE reaches N392 in N393 events, DCE will consider the errors have reached the threshold and declare the physical channels and all DLCIs to be unavailable.

N392 at DCE side should be less than N393 at DCE side.

Example # Set the operation of frame relay interface Serial 2/0 as DCE mode and set N392 to 5 and N393 to 6.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr lmi n392dce 5
[Sysname-Serial2/0] fr lmi n393dce 6
```

fr lmi n393dte

Syntax **fr lmi n393dte** *n393-value*

undo fr lmi n393dte

View Interface view

Parameter *n393-value*: The value of N393 parameter at the DTE side. It ranges from 1 to 10.

Description Use the **fr lmi n393dte** command to set N393 parameter at the DTE side.

Use the **undo fr lmi n393dte** command to restore the default.

By default, the parameter value is 4.

The DTE sends a Status-Enquiry packet at a regular interval to the DCE to inquire the link status. On receiving this packet, the DCE will immediately send a Status-Response packet. If the DTE does not receive the response packet in the specified time, it will record the error by adding 1 to the error count. If the errors exceed the threshold, the DTE will consider that the physical channels and all the DLCIs to be unavailable.

N392 and N393 together define the "error threshold". N393 indicates the event number observed and N392 indicates the error threshold of that number (N393). That is, if N392 errors occurred in N393 Status-Enquiry packets in the DTE, the DTE would consider that the error count had exceeded the threshold and declare the physical channels and all DLCIs to be unavailable.

N392 at DTE side should be less than N393 at DTE side.

Example # Set the operation of frame relay interface Serial 2/0 as the DTE mode and set N392 to 5 and N393 to 6.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dte
[Sysname-Serial2/0] fr lmi n392dte 5
[Sysname-Serial2/0] fr lmi n393dte 6
```

fr lmi t392dce

Syntax **fr lmi t392dce** *t392-value*

undo fr lmi t392dce

View Interface view

Parameter *t392-value*: Value of T392 at the DCE side. The range of the value is 5 to 30, in seconds.

Description Use the **fr lmi t392dce** command to set T392 parameter at the DCE side.

Use the **undo fr lmi t392dce** command to restore the default.

By default, the parameter value is 15 seconds.

This parameter defines the maximum time for DCE waiting for a Status-Enquiry.

T392 at DCE side should be greater than T391 at DTE side Use the **timer hold** command to configure the parameter value.

Example # Set the frame relay interface Serial 2/0 to operate in DCE mode and set T392 to 10s.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr lmi t392dce 10
```

fr lmi type

Syntax **fr lmi type** { **ansi** | **nonstandard** | **q933a** } [**bi-direction**]

undo fr lmi type

View Interface view

Parameter **ansi**: Standard LMI protocol type of ANSI T1.617 Appendix D.

nonstandard: Nonstandard compatible LMI protocol type.

q933a: Standard LMI protocol type of Q.933 Appendix A.

bi-direction: Specifies to respond to status-enquiry messages from network side in frame relay DTE mode. The support of this keyword varies with device models.

Description Use the **fr lmi type** command to configure the frame relay LMI protocol type.

Use the **undo fr lmi type** command to restore the default.

By default, the LMI protocol type is q933a.

LMI protocol is used to maintain frame relay protocol PVC table, including notifying PVC increasing, detecting PVC deleting, monitoring PVC status changing and authenticating link integrity. The system usually supports three standard LMI protocols ITU-T Q.933 Appendix A, ANSI T1.617 Appendix D, and nonstandard-compatible LMI protocol.

The **bi-direction** keyword specifies the interface to respond to status enquiry messages form network side when operating in frame relay DTE mode. It does not enable frame relay network specifications of the network side and has no effect on frame relay DCE interfaces. Normally, this keyword is only needed when the current device is to communicate with routers that require bi-directional LMI, such as Motorola Vanguard 5.3 (or former versions).

Example # Set the frame relay LIMI type of Serial 2/0 to nonstandard compatible protocol.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr lmi type nonstandard
```

fr map ip

Syntax **fr map ip** { *ip-address* [*mask*] | **default** } *dlci-number* [**broadcast** | [**nonstandard** | **ietf**] | **compression** { **frf9** | **iphc** }]*

undo fr map ip { *ip-address* | **default** } *dlci-number*

View Interface view

Parameter *ip-address*: Peer IP address.

mask: Peer IP mask, used to create a subnet address mapping.

default: Creates a default mapping.

dlci-number: Local virtual circuit number, in the range 16 to 1007.

broadcast: Specifies if broadcast packets can be sent using the map.

nonstandard: The map adopts nonstandard compatible encapsulation format. In this case, only IPHC compression can be adopted. PVC groups does not support compression.

ietf: The map adopts IETF encapsulation format. In this case, only FRF9 and IPHC can be adopted. PVC groups does not support compression.

compression: Enables frame relay compression.

frf9: Adopts payload compression.

iphc: Adopts IP, UDP, or RTP header compression.

Description Use the **fr map ip** command to add an IP address map entry for frame relay.

Use the **undo fr map ip** command to remove an IP address map entry for frame relay.

By default, no static address map entry exists and InARP is enabled.

You can create an address map manually or by using InARP. InARP is suitable for a complex network where the remote router also supports InARP. When the number of remote hosts is small or when default routes exist, however, manual map creation is preferred.

Example # Create a static address map entry on interface Serial 2/0, where DLCI 50 is connected to the router with IP address 202.38.163.252.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr map ip 202.38.163.252 50
```

fr map ppp

Syntax **fr map ppp** *dlci-number* **interface virtual-template** *interface-number*

undo fr map ppp [*dlci-number*]

View Interface view

Parameter *dlci-number*: Specific DLCI number in the range of 16 to 1007.

virtual-template *interface-number*: Virtual template interface number in the range of 0 to 1023.

Description Use the **fr map ppp** command to map the frame relay DLCI (corresponds to an Frame Relay PVC) to a PPP link, so the PPPoFR link is established, and thus PPP packets can be sent/received on FR PVC. The configuration parameter of this PPP link is up to the parameters configured on the interface specified by **interface virtual-template** *interface-number*.

Use the **undo map ppp** command to cancel this map, and thus eliminates this PPPoFR link.

Related command: **interface virtual-template** on page 1759.

Example # Map DLCI 100 to PPP and establish PPPoFR link on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr map ppp 100 interface virtual-template 1
```

fr switch

Syntax **fr switch** *name* [**interface** *interface-type interface-number* **dlci** *dlci1* **interface** *interface-type interface-number* **dlci** *dlci2*]

undo fr switch *name*

View System view

Parameter *name*: Name of a PVC used for frame relay switching, a string of 1 to 30 characters.

interface *interface-type interface-number* **dlci** *dlci1*: DLCI number at one end of PVC as well as the type and number of its interface.

interface *interface-type interface-number* **dlci** *dlci2*: DLCI number at the peer end of PVC as well as the type and number of its interface.

Description Use the **fr switch** *name* **interface** *interface-type interface-number* **dlci** *dlci1* **interface** *interface-type interface-number* **dlci** *dlci2* command to create a PVC used for frame relay switching.

Use the **fr switch** name command to enter the established frame relay switching view.

Use the **undo fr switch** command to delete a specified PVC.

By default, there is no PVC used for frame relay switching.

The interface for forwarding packets can be either a frame relay interface or an MFR interface. If Tunnel interface is specified as the forwarding interface, frame relay packets over IP can thus be realized.

In frame relay switching view, the **shutdown/undo shutdown** operation can be executed on a PVC. Before you can enter frame relay switching view, the PVC must have existed.

Example # Create a PVC named pvc1 on the DCE serving as the switch, which is from the DLCI 100 of serial interface 2/0 to the DLCI 200 of serial interface 2/1.

```
<Sysname> system-view
[Sysname] fr switching
[Sysname] fr switch pvc1 interface serial 2/0 dlci 100 interface ser
ial 2/1 dlci 200
[Sysname-fr-switching-pvc1]
```

fr switching

Syntax **fr switching**

undo fr switching

View System view

Parameter None

Description Use the **fr switching** command to enable frame relay PVC switching.

Use the **undo fr switching** command to disable frame relay PVC switching.

By default, frame relay switching is disabled.

Example # Enable PVC switching.

```
<Sysname> system-view
[Sysname] fr switching
```

interface mfr

Syntax **interface mfr** { *interface-number* | *interface-number.subnumber* }

undo interface mfr { *interface-number* | *interface-number.subnumber* }

View System view

Parameter *interface-number*: MFR interface number, in the range 0 to 1023.

interface-number.subnumber: MFR subinterface number, of which, *interface-number* is the main interface number, and *subnumber* is subinterface number. The *subnumber* argument ranges from 0 to 1023.

Description Use the **interface mfr** command to create a multilink frame relay bundle interface or subinterface and enter the corresponding interface view.

Use the **undo interface mfr** command to delete a specified multilink frame relay bundle interface or subinterface.

By default, there is no multilink frame relay interface or subinterface.

Before an MFR subinterface is created, the MFR interface must be created first.

Before using the **undo interface mfr** command to delete an MFR interface, you must delete all physical interfaces from the MFR interface.

For MFR interface, if there is one bundle link is in up state, the MFR physical state is up. Moreover, all bundle links should be tagged as down before the bundle is down. The link layer protocol on MFR interface is determined by LMI packet negotiation.

Example # Create a multilink frame relay bundle interface MFR4 with a point-to-multipoint subinterface.

```
<Sysname> system-view
[Sysname] interface mfr 4
[Sysname-MFR4] quit
[Sysname] interface mfr 4.1
[Sysname-MFR4.1]
```

interface serial

Syntax **interface serial** *interface-number.subnumber* [**p2p** | **p2mp**]

undo interface serial *interface-number.subnumber*

View System view

Parameter *interface-number*: Main interface number.

subnumber: Subinterface number, in the range 0 to 1023.

p2p: Specifies a point-to-point subinterface.

p2mp: Specifies a point-to-multipoint subinterface.

Description Use the **interface serial** command to create subinterface and enter subinterface view.

Use the **undo interface serial** command to delete subinterface.

Frame relay subinterface type defaults to **p2mp**.

Example # Configure a point-to-point subinterface Serial 2/0.2.

```
<Sysname> system-view
[Sysname] interface serial2/0.2 p2p
[Sysname-Serial2/0.2]
```

link-protocol fr

Syntax **link-protocol fr** [**ietf** | **nonstandard**]

View Interface view

Parameter **ietf**: Internet Engineering Task Force (IETF) standard encapsulation format (default).

nonstandard: Nonstandard compatible encapsulation format.

Description Use the **link-protocol fr** command to encapsulate interface link layer protocol as frame relay.

By default, the link-layer protocol encapsulated on the interface is PPP.

The frame relay encapsulation can be either **ietf** or **nonstandard**. IETF encapsulation conforms to RFC 1490, that is, it supports the IETF standard and is compatible with dedicated encapsulation format of mainstream routers.

If you encapsulate a frame relay interface using any of the above frame relay formats, the packets are encapsulated in the corresponding frame relay format before they are forwarded through the interface. That is, two devices can communicate with each other if the interfaces of both sides can recognize packets in both of the formats even if they are encapsulated using different frame relay formats. If an interface on one side cannot recognize packets of both formats, you need to encapsulate the two interfaces using the same frame relay format.

Example # Configure frame relay encapsulation on interface Serial 2/0 and select the nonstandard encapsulation compatible format.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol fr nonstandard
```

link-protocol fr mfr

Syntax **link-protocol fr mfr** *interface-number*

View Interface view

Parameter *interface-number*: MFR interface number, in the range 0 to 1023.

Description Use the **link-protocol fr mfr** command to configure the current physical interface as an MFR bundle link and bind it to an MFR interface.

By default, an interface is not bound to any MFR interface.

Note that:

- When this command is configured, the specified MFR interface must exist. A maximum of 16 physical interfaces can be bundled onto an MFR interface.
- To delete a physical interface from an MFR interface, use the **link-protocol** command to apply a link layer protocol of non frame relay MFR to the interface.
- After a physical interface is encapsulated as MFR format, the interface belongs to MFR and is not allowed to be configured using the commands related to FR except MFR. In addition, the queue type on the interface can be configured as FIFO (first in first out) only even if the other queue types have been encapsulated on the interface, they would be converted to FIFO type by force.

Example # Configure Serial 2/0 as a bundle link and add it onto the Frame Relay bundle interface MFR4.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol fr mfr 4
```

mfr bundle-name

Syntax **mfr bundle-name** [*name*]

undo mfr bundle-name

View MFR interface view

Parameter *name*: Bundle identification, a string of 1 to 49 characters.

Description Use the **mfr bundle-name** command to set frame relay bundle identification (BID).

Use the **undo mfr bundle-name** command to restore the default.

By default, BID is represented by mfr plus frame relay bundle number, for example, mfr4.

Each MFR bundle has a BID, which only has local significance. Therefore, the same BID can be used at both ends of the link.

Note that:

- In spite of the default BID, you cannot configure a BID as a string in the form of **mfr** + number.
- After changing the BID of an MFR interface, you must execute the **shutdown** and **undo shutdown** command on the interface to validate the new BID.

Example # Set the frame relay link MFR4 BID to bundle1.

```
<Sysname> system-view
[Sysname] interface mfr 4
[Sysname-MFR4] mfr bundle-name bundle1
```

mfr fragment

Syntax **mfr fragment**

undo mfr fragment

View MFR interface view

Parameter None

Description Use the **mfr fragment** command to enable fragmentation on the MFR bundle.

Use the **undo mfr fragment** command to disable the function.

By default, fragmentation is disabled on the MFR bundle.

Example # Enable fragmentation on interface MFR 4.

```
<Sysname> system-view
[Sysname] interface mfr 4
[Sysname-MFR4] mfr fragment
```

mfr fragment-size

Syntax **mfr fragment-size** *bytes*

undo mfr fragment-size

View Frame relay interface view and MFR interface view

Parameter *bytes*: Fragment size, ranging from 60 to 1,500 in bytes.

Description Use the **mfr fragment-size** command to configure the maximum fragment size allowed on a frame relay bundle link.

Use the **undo mfr fragment-size** command to restore the default.

By default, the maximum fragment size allowed on a frame relay bundle link is of 300 bytes.

The bundle link executes the priority of the fragment size configured on the frame relay interface view after the fragmentation is enabled on MFR interface. If the frame relay interface view is not configured with fragment size, use the fragment size configured on MFR interface view. The priority of the fragment size configured in frame relay interface view is higher than that of the one configured in MFR interface view.

Example # Configure the maximum fragment size allowed on the multilink frame relay bundle link Serial 2/0 to be 70 bytes.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mfr fragment-size 70
```

mfr link-name

Syntax **mfr link-name** [*name*]

undo mfr link-name [*name*]

View Frame relay interface view

Parameter *name*: Name of a bundle link identification, a string of 1 to 49 characters.

Description Use the **mfr link-name** command to set the frame relay bundle link identification (LID).

Use the **undo mfr link-name** command to restore the default.

By default, LID is the name of the corresponding physical interface.

Use the **link-protocol fr mfr** command to configure the current physical interface as a multilink frame relay bundle link before using the **mfr link-name** command to configure. The peer equipment identifies a frame relay bundle link via LID or associates the bundle link with a frame relay bundle by using LID. LID is locally valid; therefore, the LIDs at both ends of a link can be the same.

When changing the bundle LID on an interface, you must execute the **shutdown/undo shutdown** command on the interface to make the new bundle LID valid.

Example # Set the bundle LID of the multilink frame relay bundle link Serial 2/0 to be bl1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mfr link-name bl1
```

mfr retry

Syntax **mfr retry** *number*

undo mfr retry

View Frame relay interface view

Parameter *number*: The maximum times that a bundle link can resend hello messages, in the range 1 to 5.

Description Use the **mfr retry** command to set the maximum times that a frame relay bundle link can resend hello message when waiting for a hello acknowledgement message.

Use the **undo mfr retry** command to restore the default.

By default, the maximum times that a frame relay bundle link can resend hello message is twice.

The bundle link sustains link status by periodically sending hello message to the peer end. If the times that a bundle link resends hello message reach the maximum without receiving acknowledgement from the peer, the system will regard the link protocol on the bundle link to be malfunctioning.

Only after the **link-protocol fr mfr** command is used to associate a frame relay bundle link interface with a frame relay bundle, can this command be configured.

Example # Set the bundle link Serial 2/0 to resend hello message for 3 times at most.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mfr retry 3
```

mfr stateup-respond-addlink

Syntax **mfr stateup-respond-addlink**

undo mfr stateup-respond-addlink

View System view

Parameter None

Description Use the **mfr stateup-respond-addlink** command to configure an MFR interface to return ADD_LINK messages and transit the corresponding physical interface to the protocol ADD_SENT state when it is in protocol up state and receives an ADD_LINK request from the peer.

Use the **undo mfr stateup-respond-addlink** command to restore the default.

By default, an MFR interface does not respond to ADD_LINK requests received even if it is in protocol up state. This causes the peer port cannot be in protocol up state.

Example # Configure the MFR interface to return ADD_LINK messages and transit the corresponding physical interface to the protocol ADD_SENT state when it is in protocol up state and receives an ADD_LINK request from the peer.

```
<Sysname> system-view
[Sysname] mfr stateup-respond-addlink
```

mfr timer ack

Syntax **mfr timer ack** *seconds*

undo mfr timer ack

View Frame relay interface view

Parameter *seconds*: Time (in seconds) of waiting for hello acknowledgment message before resending hello message, in the range 1 to 10.

Description Use the **mfr timer ack** command to set the time of waiting for hello acknowledgment message before frame relay bundle link resends hello message.

Use the **undo mfr timer ack** command to restore the default.

By default, time of waiting for hello acknowledgment message before resending hello message is 4 seconds.

The bundle link sustains link status by periodically sending hello message to the peer end. If the times that a bundle link resends hello message reach the maximum without receiving acknowledgement from the peer, the system will regard the link protocol on the bundle link to be malfunctioning.

Only after the **link-protocol fr mfr** command is used to associate a frame relay bundle link interface with a frame relay bundle, can this command be configured.

Related command: **mfr timer hello**, **mfr retry**.

Example # Set the frame relay bundle link Serial 2/0 to wait for six seconds before resending hello message.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mfr timer ack 6
```

mfr timer hello

Syntax **mfr timer hello** *seconds*

undo mfr timer hello

View Frame relay interface view

Parameter *seconds*: Interval (in seconds) for a bundle link to send hello message, in the range 1 to 180.

Description Use the **mfr timer hello** command to set the interval for a frame relay bundle link to send hello message.

Use the **undo mfr timer hello** command to restore the default.

By default, the interval for a frame relay bundle link to send hello message is 10 seconds.

Only after the **link-protocol fr mfr** command is used to associate a frame relay bundle link interface with a frame relay bundle, can this command be configured.

Example # Set the bundle link Serial 2/0 to send hello message once every 15 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mfr timer hello 15
```

mfr window-size

Syntax **mfr window-size** *number*

undo mfr window-size

View MFR interface view

Parameter *number*: Number of fragments, in the range 1 to 16.

Description Use the **mfr window-size** command to configure the number of fragments that can be hold by the window used in sliding window algorithm when multilink frame relay reassembles received fragments.

Use the **undo mfr window-size** command to restore the default.

By default, the size of a sliding window is equal to the number of physical interfaces of an MFR bundle.

Example # Set the size of the sliding window of the MFR bundle interface MFR4 to be 8.

```
<Sysname> system-view
[Sysname] interface mfr 4
[Sysname-MFR4] mfr window-size 8
```

shutdown

Syntax **shutdown**

undo shutdown

View Frame relay switching view

Parameter None

Description Use the **shutdown** command to disable the current switching PVC.

Use the **undo shutdown** command to enable the current switching PVC.

By default, the switching PVC is enabled.

Example # Create a PVC named pvc1 on the DCE serving as the switch, which is from the DLCI 100 of Serial 2/0 to the DLCI 200 of Serial 2/1 and disable the current switching PVC.

```
<Sysname> system-view
[Sysname] fr switching
[Sysname] fr switch pvc1 interface serial 2/0 dlci 100 interface ser
ial 2/1 dlci 200
[Sysname-fr-switching-pvc1] shutdown
```

reset fr inarp

Syntax **reset fr inarp**

View User view

Parameter None

Description Use the **reset fr inarp** command to clear the address mapping established by inverse ARP.

In some special cases, for example, when the network architecture changes, the dynamic address maps originally established will become invalid. Hence it is necessary to establish them again. Users can use this command to clear all the dynamic address maps.

Related command: **fr inarp**.

Example # Clear all the frame relay dynamic address maps.

```
<Sysname> reset fr inarp
```

reset fr pvc

Syntax **reset fr pvc interface serial** *interface-number* [**dlci** *dlci-number*]

View User view

Parameter *interface-number*: Interface number.

dlci *dlci-number*: DLCI assigned to an FR interface. The *dlci-number* argument is in the range 16 to 1007. Note that DLCI 0 through 15 and 1008 through 1023 are reserved for special use and are thus unavailable.

Description Use the **reset fr pvc** command to clear the statistics on a PVC.

Example # Clear PVC statistics on Serial 2/0.

```
<Sysname> reset fr pvc interface serial 2/0
```

timer hold

Syntax **timer hold** *seconds*

undo timer hold

View Interface view

Parameter *seconds*: Value of T391 parameter at DTE side, which ranges from 0 to 32767 in seconds. 0 indicates that the LMI protocol is disabled.

Description Use the **timer hold** command to configure T391 parameter at the DTE side.

Use the **undo timer hold** command to restore the default.

By default, the parameter is 10 seconds.

The parameter is a time variable that defines the interval of Status-Enquiry packet sent by DTE.

Related command: **fr lmi t392dce**.

Example # Configure that frame relay interface Serial 2/0 to operate in DTE mode, and set the value of T391 parameter to 15 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol fr
```

```
[Sysname-Serial2/0] fr interface-type dte
[Sysname-Serial2/0] timer hold 15
```

x25-template

Syntax **x25-template** *name*

undo x25-template *name*

View DLCI interface view

Parameter *Name*: Name of an X.25 template, a string of 1 to 30 characters.

Description Use the **x25-template** command to apply an X.25 template to a VC.

Use the **undo x25-template** command to remove the X.25 template applied to a VC.

Annex G implements X.25 over FR. You can configure X.25 parameters for an X.25 over FR DLCI using the **x25 template** command and apply the template in DLCI interface view.

Example # Apply the X.25 template named "vofr" to DLCI 100.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] fr dlci 100
[Sysname-fr-dlci-Serial2/0-100] x25-template vofr
```

x25 template

Syntax **x25 template** *name*

undo x25 template *name*

View System view

Parameter *Name*: Name of an X.25 template, a string of 1 to 30 characters.

Description Use the **x25 template** command to create an X.25 template or enter X.25 template view.

Use the **undo x25 template** command to remove an X.25 template.

As for the **x25 template** command, if the X.25 template identified by the *name* argument already exists, this command leads you to X.25 template view. X.25-/LAPB-related parameters are configured in X.25 template view.

Example # Create an X.25 template named "vofr".

```
<Sysname> system-view
[Sysname] x25 template vofr
[Sysname-x25-vofr]
```

23 GARP CONFIGURATION COMMANDS

display garp statistics

Syntax **display garp statistics** [**interface** *interface-list*]

View Any view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp statistics** command to display the GARP statistics of the specified or all ports.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP statistics of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command displays the GARP statistics of the specified ports.

Example # Display statistics about GARP for port Ethernet 1/0.

```
<Sysname> display garp statistics interface ethernet1/0
        GARP statistics on port Ethernet1/0

        Number of GVRP Frames Received          : 0
        Number of GVRP Frames Transmitted       : 0
        Number of Frames Discarded              : 0
```

display garp timer

Syntax **display garp timer** [**interface** *interface-list*]

View Any view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range

defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display garp timer** command to display GARP timers.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command displays the GARP timer settings of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command displays the GARP timer settings of the specified ports.

Related command: **garp timer**, **garp timer leaveall**.

Example # Display GARP timers on port Ethernet 1/0.

```
<Sysname> display garp timer interface ethernet 1/0
        GARP timers on port Ethernet1/0

                Garp Join Time          : 20 centiseconds
                Garp Leave Time         : 60 centiseconds
                Garp LeaveAll Time      : 1000 centiseconds
                Garp Hold Time          : 10 centiseconds
```

garp timer

Syntax **garp timer** { **hold** | **join** | **leave** } *timer-value*

undo garp timer { **hold** | **join** | **leave** }

View Ethernet interface view, port group view

Parameter **hold**: Sets the hold timer.

join: Sets the join timer.

leave: Sets the leave timer.

timer-value: Timer setting (in centiseconds), which must be a multiple of 5.

Description Use the **garp timer** command to set a GARP timer for an Ethernet port or all ports in a port group in compliance with the timer setting dependencies shown in Table 53.

Use the **undo garp timer** command to restore the default of a GARP timer. This may fail if the default does not satisfy the dependencies shown in Table 53.

By default, the hold timer, the join timer, and the leave timer are set to 10 centiseconds, 20 centiseconds, and 60 centiseconds.

When restoring the default GARP timers, you are recommended to do that on the timers in the order of hold, join, leave, and leaveall.

When configuring GARP timers, note that their values are dependent on each other and must be a multiplier of five centiseconds. If the value range for a timer is not desired, you may change it by tuning the value of another timer as shown in the following table:

Table 53 Dependencies of GARP timers

Timer	Lower limit	Upper limit
Hold	10 centiseconds	Not greater than half of the join timer setting
Join	Not less than two times the hold timer setting	Less than half of the leave timer setting
Leave	Greater than two times the join timer setting	Less than the leaveall timer setting
Leaveall	Greater than the leave timer setting	32765 centiseconds

Related command: **display garp timer**.

Example # Set the GARP join timer to 25 centiseconds, assuming that both the hold timer and the leave timer are using the default.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] garp timer join 25
```

garp timer leaveall

Syntax **garp timer leaveall** *timer-value*

undo garp timer leaveall

View System view

Parameter *timer-value*: Leaveall timer setting, in the range 65 to 32765 (in centiseconds). Note that the setting of the leaveall timer must be a multiple of 5 and must be greater than the leave timer settings of all the ports.

Description Use the **garp timer leaveall** command to set the leaveall timer of GARP.

Use the **undo garp timer leaveall** command to restore the default. This may fail if the default is less than the setting of the current leave timer.

By default, the setting of the leaveall timer is 1000 centiseconds (that is, 10 seconds).

A leaveall timer starts upon the start of a GARP application entity. When this timer expires, the entity sends a LeaveAll message so that other entities can re-register its attribute information and starts another leaveall timer at the same time.

Each time a device on the network receives a LeaveAll message, it resets its leaveall timer. Therefore, a GARP application entity may send LeaveAll messages at the interval set by its leaveall timer or the leaveall timer on another device on the network, whichever is smaller.

Related command: **display garp timer**.

Example # Set the leaveall timer to 100 centiseconds, assuming that the leave timer is 60 centiseconds.

```
<Sysname> system-view
[Sysname] garp timer leaveall 100
```

reset garp statistics

Syntax **reset garp statistics** [**interface** *interface-list*]

View User view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **reset garp statistics** command to clear GARP statistics of the specified or all ports.

Note that:

- If the **interface** *interface-list* keyword-argument combination is not specified, this command clears the GARP statistics of all the ports.
- If the **interface** *interface-list* keyword-argument combination is specified, this command clears the GARP statistics of the specified ports.

Related command: **display gvrp statistics**.

Example # Clear statistics about GARP on all ports.

```
<Sysname> reset garp statistics
```

24 GVRP CONFIGURATION COMMANDS

display gvrp statistics

Syntax **display gvrp statistics** [**interface** *interface-list*]

View Any view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **display gvrp statistics** command to display GVRP statistics of the specified or all trunk ports.

Note that if the **interface** *interface-list* is not provided, the GVRP statistics of all trunk ports will be displayed. Otherwise, only the GVRP statistics of all the specified trunk port will be displayed.

Example # Display statistics about GVRP for trunk port Ethernet 1/0.

```
<Sysname> display gvrp statistics interface ethernet 1/0
        GVRP statistics on port Ethernet1/0

                GVRP Status                     : Enabled
                GVRP Running                    : YES
                GVRP Failed Registrations       : 0
                GVRP Last Pdu Origin            : 0000-0000-0000
                GVRP Registration Type          : Normal
```

Table 54 Description on the fields of the display gvrp statistics command

Field	Description
GVRP Status	Indicates whether GVRP is enabled or disabled.
GVRP Running	Indicates whether GVRP is running.
GVRP Failed Registrations	Indicates the number of GVRP registration failures.
GVRP Last Pdu Origin	Indicates the source MAC address in the last GVRP PDU.
GVRP Registration Type	Indicates the GVRP registration type on the port.

display gvrp status

Syntax **display gvrp status**

View Any view

Parameter None

Description Use the **display gvrp status** command to display the global enable/disable state of GVRP.

Example # Display the global GVRP enable/disable state.

```
<Sysname> display gvrp status
GVRP is enabled
```

gvrp

Syntax **gvrp**

undo gvrp

View System view, Ethernet interface view, port group view

Parameter None

Description Use the **gvrp** command to enable GVRP.

Use the **undo gvrp** command to disable GVRP.

Disabling GVRP globally also disables it on all ports.

By default, GVRP is disabled.

Configured in system view, the setting is globally effective; configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

- *To enable GVRP on a port, you need to enable it globally.*
- *The port where you enable/disable GVRP must be a trunk port.*

Related command: **display gvrp status**.

Example # Enable GVRP globally.

```
<Sysname> system-view
[Sysname] gvrp
GVRP is enabled globally.
```

gvrp registration

Syntax **gvrp registration** { **fixed** | **forbidden** | **normal** }

undo gvrp registration

View Ethernet interface view, port group view

Parameter **fixed**: Sets the registration type to fixed.

forbidden: Sets the registration type to forbidden.

normal: Sets the registration type to normal.

Description Use the **gvrp registration** command to configure the GVRP registration type on a port.

Use the **undo gvrp registration** command to restore the default.

The default GVRP registration type is normal.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

GVRP provides the following three registration types on a port:

- Normal -- Enables the port to dynamically register/deregister VLANs, and to propagate both dynamic and static VLAN information.
- Fixed -- Disables the port to dynamically register and deregister VLANs or propagate information about dynamic VLANs, but allows the port to propagate information about static VLANs. A trunk port with fixed registration type thus allows only manually configured VLANs to pass through even though it is configured to carry all VLANs.
- Forbidden -- Disables the port to dynamically register and deregister VLANs, and to propagate VLAN information except information about VLAN 1. A trunk port with forbidden registration type thus allows only VLAN 1 to pass through even though it is configured to carry all VLANs.

Note that this command is only available on trunk ports.

Related command: **display garp statistics**.

Example # Set the GVRP registration type to fixed on port Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type trunk
[Sysname-Ethernet1/0] gvrp registration fixed
```

25 HDLC CONFIGURATION COMMANDS

link-protocol hdlc

Syntax **link-protocol hdlc**

View Interface view

Parameter None

Description Use the **link-protocol hdlc** command to configure HDLC encapsulation on the interface.

As a data link layer protocol, HDLC can carry network layer protocols, such as IP and IPX.

By default, PPP encapsulation is configured on an interface.

Related command: **timer hold**

Example # Configure HDLC encapsulation on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol hdlc
```

timer hold

Syntax **timer hold** *seconds*

undo timer hold

View Interface view

Parameter *seconds*: Link status polling interval (in seconds), in the range 0 to 32767.

Description Use the **timer hold** command to set the polling interval.

Use the **undo timer hold** command to restore the default.

By default, the link status polling interval is 10 seconds on the interface.

You should set the same polling interval on both the local and remote devices. Setting it to zero disables link status check.

Example # Set the link status polling interval to 100 seconds on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] timer hold 100
```

26 LAPB AND X.25 CONFIGURATION COMMANDS

channel

Syntax **channel** { **interface** *interface-type interface-number* [**dlci** *dlci-number*] | **xot** *ip-address* }

undo channel { **interface** *interface-type interface-number* | **xot** *ip-address* }

View X.25 hunt group view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

dlci *dlci-number*: Specifies an FR DLCI. The *dlci-number* argument is in the range of 16 to 1007.

xot *ip-address*: Specifies the IP address of the peer XOT host.

Description Use the **channel** command to add an X.25 interface, Annex G DLCI or XOT channel to the current hunt group.

Use the **undo channel** command to remove the specified interface, Annex G DLCI or XOT channel from the current hunt group.

Related command: **x25 hunt-group**.

Example # Add serial2/0 to the hunt group hg1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25
[Sysname-Serial2/0] x25 x121-address 1111
[Sysname-Serial2/0] quit
[Sysname] x25 hunt-group hg1 round-robin
[Sysname-hg-hg1] channel interface serial 2/0
```

Add Annex DLCI 100 to the hunt group hg1.

```
<Sysname> system-view
[Sysname] interface serial 2/1
[Sysname-Serial2/1] link-protocol fr
[Sysname-Serial2/1] fr dlci 100
[Sysname-fr-dlci-Serial2/1-100] annexg dce
[Sysname-fr-dlci-Serial2/1-100] quit
```

```
[Sysname-Serial2/1] quit
[Sysname] x25 hunt-group hg1 round-robin
[Sysname-hg-hg1] channel interface serial 2/1 dlci 100
```

Add the XOT channel with a destination of 10.1.1.2 to hunt group hg1.

```
<Sysname> system-view
[Sysname] x25 hunt-group hg1 round-robin
[Sysname-hg-hg1] channel xot 10.1.1.2
```

display interface

Syntax **display interface** [*interface-type* [*interface-number*]]

View Any view

Parameter *interface-type* [*interface-number*]: Specifies an interface by its type and number.

Description Use the **display interface** command to view the interface information.

Example # Encapsulate Serial2/0 with X.25 protocol and view the interface information.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] link-protocol x25 dce
[Sysname-Serial2/0] display interface serial 2/0
Serial2/0 current state: UP
Line protocol current state: UP
Description: Serial2/0 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
  Link-protocol is X.25 DCE Ietf, address is , state R1, modulo 8
    window sizes input:2 output:2, packet sizes input:128 output:128
    Channels: Incoming-only 0-0, Two-way 1-1024, Outgoing-only 0-0
    Timers: T10 60, T11 180, T12 60, T13 60, Idle_Timer 0 (seconds)
      New configuration(will be effective after restart): modulo 8
        window sizes input:2 output:2, packet sizes input:128 output:128
        Channels: Incoming-only 0-0, Two-way 1-1024, Outgoing-only 0-0
    Statistic: Restarts 0 (Restart Collisions 0)
      Refused Incoming Call 0, Failing Outgoing Call 0
      input/output: RESTART 1/1  CALL 0/0  DIAGNOSE 0/0
                    DATA 0/0  INTERRUPT 0/0  Bytes 0/0
                    RR 0/0  RNR 0/0  REJ  0/0
      Invalid Pr: 0  Invalid Ps: 0  Unknown: 0
Link-protocol is LAPB
  LAPB DCE, module 8, window-size 7, max-frame 12056, retry 10
  Timer:  T1 3000,  T2 1500, T3 0  (milliseconds),  X.25-protocol
  state CONNECT, VS 1, VR 1, Remote VR 1
  IFRAME 1/1, RR 1/1, RNR 0/0, REJ 0/0
  FRMR 0/0, SABM 0/1, DM 0/0, UA 1/0
  DISC 0/0, invalid ns 0, invalid nr 0, link resets 0
Output queue : (Urgent queuing : Size/Length/Discards)  0/50/0
Output queue : (Protocol queuing : Length)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Physical layer is synchronous, Baudrate is 64000 bps
Interface is DCE, Cable type is V35, Clock mode is DCECLK
Last clearing of counters: Never
    Last 300 seconds input rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Last 300 seconds output rate 0.00 bytes/sec, 0 bits/sec, 0.00 packets/sec
    Input: 208 packets, 6329 bytes
```

```
        0 broadcasts, 0 multicasts
        3 errors, 0 runts, 0 giants
        0 CRC, 3 align errors, 0 overruns
        0 dribbles, 0 aborts, 0 no buffers
        0 frame errors
Output:210 packets, 4720 bytes
        0 errors, 0 underruns, 0 collisions
        0 deferred
DCD=UP  DTR=UP  DSR=UP  RTS=UP  CTS=UP
```

Table 55 Description on the fields of the display interface command

Field	Description
Link-protocol is X.25 DCE Ietf	Current encapsulation protocol of this interface is X.25 protocol that works in DCE mode, and the data packet encapsulation format is IETF.
address is	X.121 address of this X.25 interface; this field will be empty if there is no address.
state	Current status of this X.25 interface.
modulo	Data packets and traffic control packets sent by this X.25 interface are numbered in modulo 8 mode.
window sizes input:2 output:2, packet sizes input:128 output:128	Flow control parameters of this X.25 interface, including receiving window size, sending window size, maximum received packet size (in bytes), and maximum sent packet size (in bytes).
Channels: Incoming-only 0-0, Two-way 1-1024, Outgoing-only 0-0	Channel range division of this X.25 interface, sequentially as incoming-only channel section, two-way channel section, outgoing-only channel section; if both demarcating values of an section are 0, this section is disabled.
Timers: T20 180, T21 200, T22 180, T23 180, T28 300, Idle_Timer 0 <seconds>	Delay values of various timers of this X.25 interface, in seconds
New Configuration:	New configuration of this X.25 interface taking effect after next restart; if this configuration is wrong, the default value will be restored
Restarts 0 (Restart Collisions 0)	Statistics of this X.25 interface, including times of restart (including restart collision)
Refused Incoming Call	Statistics information of this X.25 interface: times of call refusals
Failing Outgoing Call	Statistics information of this X.25 interface: Number of failed outgoing calls.
input/output: RESTART 1/1 ... REJ 0/0	Statistics information of this X.25 interface: quantities of received and sent packets, format: received quantity/sent quantity.
Invalid Pr	Error statistics information of this X.25 interface: total of received data packets and traffic control packets carrying erroneous acknowledgement numbers.
Invalid Ps	Error statistics information of this X.25 interface: total of received data packets carrying erroneous sequence numbers.
Unknown	Error statistics information of this X.25 interface: total of received irresolvable packets.
Link-protocol is LAPB	Current encapsulation protocol of this interface is LAPB protocol.
LAPB DCE:	LAPB of this interface works in DCE mode.
module 8	Information frame and monitoring frame sent by this interface LAPB are numbered in the modulo 8 view.

Table 55 Description on the fields of the display interface command

Field	Description
window-size 7	Window size of this interface LAPB is 7.
max-frame 12056	The maximum length of frame sent by the interface LAPB is 12056 bits.
retry 10	Maximum re-sending times of information frame of this interface LAPB is 10.
timer	Delay value of timers of this interface LAPB, in milliseconds. The unit of T3 is second.
state	Current status of this interface LAPB.
VS	Sending variable of this interface LAPB.
VR	Receiving variable of this interface LAPB.
Remote VR	Peer's last acknowledgment on information frame received by this interface LAPB.
IFRAME 147/254 ... DISC 0/0	Statistics information of frames sent and received by this interface LAPB, format: received quantity/sent quantity.
invalid ns	Error statistics of this interface LAPB, including total of received information frames carrying erroneous sequence numbers.
invalid nr	Error statistics of this interface LAPB, including total of received information frames and monitoring frames carrying erroneous acknowledgment numbers.
link resets	Restarting times of this interface LAPB link.
Physical layer is synchronous	Physical layer is synchronous
Baudrate is 64000 bps	Baudrate is 64000 bps on the interface
Interface is DCE, Cable type is V35, Clock mode is DCECLK	Interface is DCE, Cable type is V35, Clock mode is DCECLK
Last clearing of counters: Never	Counters has never been removed
Last 300 seconds input rate	Average input rate in last 300 seconds
Last 300 seconds output rate	Average output rate in last 300 seconds
Input	Input packets
Output	Output packets
DCD	Data carrier detection
DTR	Data terminal ready
DSR	Data set ready
RTS	Request to send
CTS	Clear to send

display x25 alias-policy

Syntax **display x25 alias-policy** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display x25 alias-policy** command to view X.25 alias table.

Related command: **x25 alias-policy**.

Example # Display X.25 alias table.

```
<Sysname> display x25 alias-policy
Alias for interface Serial2/1:
Alias for interface Serial2/0:
    Alias-1:   $20112405$         strict
    Alias-2:   $20112450          left
    Alias-3:   20112450$          right
```

display x25 cug

Syntax **display x25 cug** { **local-cug** [*local-cug-number*] | **network-cug** [*network-cug-number*] }

View Any view

Parameter **local-cug** [*local-cug-number*]: Specifies a local CUG.

network-cug [*network-cug-number*]: Specifies a network side CUG.

Description Use the **display x25 cug** command to display the CUG configuration on the router ports.

Example # Display the CUG configuration on the router ports.

```
<Sysname> display x25 cug local-cug
X.25 Serial2/0, 2 CUGs subscribed with no public access
           local-cug    1 <-> network-cug 4    , no-incoming
           local-cug    2 <-> network-cug 5    , preferentiallocal-cug    3
<-> network-cug 5   , preferential
```

Table 56 Description on the fields of the display x25 cug command

Field	Description
X.25 Serial2/0, 2 CUGs subscribed with no public access	Name of the interface, where two CUG mappings are configured and no incoming/outgoing access policy is configured.
local-cug 2 <-> network-cug 4	Local CUG 2 is mapped to network CUG 4
no-incoming, preferential	Suppression rule: no-incoming indicates income access is prohibited, and preferential indicates the mapping is a preference rule.

display x25 hunt-group-info

Syntax **display x25 hunt-group-info** [*hunt-group-name*]

View Any view

Parameter *hunt-group-name*: Hunt group name, a string of 1 to 30 characters.

Description Use the **display x25 hunt-group-info** command to view the status information of X.25 hunt group.

You can use this command to learn the hunt group of the Router and the information about the interfaces and XOT channel inside the hunt group.

Related command: **x25 hunt-group**.

Example # Display the status information of X.25 hunt group hg1.

```
<Sysname> display x25 hunt-group-info hg1
HG_ID : hg1    HG_Type: round-robin
member      state       vc-used   in-pkts   out-pkts
Serial1/0   Last used   2         51        20
Serial2/0   Next        1         21        15
1.1.1.1     Normal      1         24        3
```

Table 57 Description on the fields of the display x25 hunt-group-info command

Field	Description
HG_ID : hg1	The hunt group name is hg1
HG_Type: round-robin	Hunt group call channel selection policy (including round-robin and vc-number)
member	Interfaces or XOT channel contained in hunt group
state	The state of the current interface or XOT channel, including:
	Last used: latest used
	Next: next selected
	Normal: normal state
	Unavail: Unavailable state
vc-used	Number of calls on the interface or XOT channel (including call success and call failure)
in-pkts	Input flow on the interface or XOT channel in packets
out-pkts	Output flow on the interface or XOT channel in packets

display x25 map

Syntax **display x25 map**

View Any view

Parameter None

Description Use the **display x25 map** command to display the X.25 address mapping table.

The X.25 address mapping can be configured in two methods: using the **x25 map** command or using the **x25 pvc** command. The **display x25 map** command can display all the address mappings.

Example # Display the X.25 address mapping table.

```
<Sysname> display x25 map
Interface:Serial3/0(protocol status is up):
ip address:202.38.162.2   X.121 address: 22
    map-type: SVC_MAP  VC-number: 0
    Facility:
      ACCEPT_REVERSE;
      BROADCAST;
      PACKET_SIZE: I 512  O 512
```

Table 58 Description on the fields of the display x25 map command

Field	Description
Interface:Serial3/0(protocol status is up)	Interface name and protocol status
ip address:202.38.162.2 X.121 address: 22	IP address and X.121 address of the interface
map-type: SVC_MAP	Mapping type
VC-number: 0	VC number
Facility:	User facility of the interface

display x25 pad

Syntax **display x25 pad** [*pad-id*]

View Any view

Parameter *pad-id*: X.25 PAD connection (packet assembly/disassembly facility). The ID is in the range 0 to 255.

Description Use the **display x25 pad** command to display X.25 PAD connection information.

If no pad ID is specified, all PAD connection information will be displayed.

Example # Display all X.25 PAD connection information.

```
<Sysname> display x25 pad
  UI-INDEX130:
  From remote 22 connected to local 11, State: Normal
  X.3Parameters(In):
 1:1,2:0,3:2,4:1,5:0,6:0,7:21,8:0,9:0,10:0,11:14
12:0,13:0,14:0,15:0,16:127,17:21,18:18,19:0,20:0,21:0,22:0
  X.3Parameters(Out):
1:1,2:0,3:2,4:1,5:0,6:0,7:21,8:0,9:0,10:0,11:14
12:0,13:0,14:0,15:0,16:127,17:21,18:18,19:0,20:0,21:0,22:0
Input:
Pkts(total/control): 13/2  bytes:12
queue(size/max) :0/200
Output:
Pkts(total/control): 15/2  bytes:320
```

Table 59 Description on the fields of the display x25 pad command

Field	Description
UI-INDEX130:	User interface index
From remote 22 connected to local 11, State: Normal	Connection of local X.121 address to remote X.121 address and the current connection state of the PAD.
	Connection states:
	Normal: Connection is normal
	Closing: Connection is being closed
	Exception: Connection is abnormal
X.3Parameters(In):	Incoming X.3 parameter
X.3Parameters(Out):	Outgoing X.3 parameter
Input: Pkts(total/control): 13/2	Total number of packets received/total number of control packets received
bytes:12	Total size of packets received
queue(size/max) :0/200	Size/maximum size of receiving queue packets
Output:	Total number of packets sent/total number of control packets sent
Pkts(total/control): 15/2 bytes:320	Size of packets sent

display x25 switch-table pvc

Syntax **display x25 switch-table pvc**

View Any view

Parameter None

Description Use the **display x25 switch-table pvc** command to display X.25 PVC switching table.

Example # Display X.25 PVC switching table.

```
<Sysname> display x25 switch-table pvc
#1  (In: Serial1/1-vc1024)<- ->(Out: Serial1/0-vc1)
#2  (In: Serial1/0-vc1024)<- ->(Out: Serial1/1-vc1)
```

Table 60 Description on the fields of the display x25 switch-table pvc command

Field	Description
(In: Serial1/1-vc1024)<- ->(Out: Serial1/0-vc1)	Data is exchanged between PVC 1024 of Serial 1/1 and PVC 1 of Serial 1/0.

display x25 switch-table svc

Syntax **display x25 switch-table svc** { **dynamic** | **static** }

View Any view

Parameter **dynamic**: Displays VC switching table.

static: Displays SVC switching table.

Description Use the **display x25 switch-table svc** command to display SVC switching table.

With the keyword **static** included, the manually configured SVC switching table is displayed.

With the keyword **dynamic** included, the VC switching table is displayed. VC routing table is the link relationship between the node port number and the logic channel number of the VC. VC routing table changes with calls: it is generated as a call is established and it is cleared as the call is over.

Related command: **x25 switch svc**.

Example # Display X.25 SVC static switching table.

```
<Sysname> display x25 switch-table svc static
Number Destination  Substitute-src Substitute-dst CUD   SwitchTo(type/name)
1      11                                           I/Serial2/0
2      22                                           I/Serial2/1/0
3      131                                          H/hg1
4      132                                          T/123.123.123.123
5      133                                          T/123.123.123.123
6      111          222            333              T/4.4.4.4
Total of static svc is 6.
The item type of SwitchTo meaning:
I: interface   H: hunt-group   T: xot
```

Table 61 Description on the fields of the display x25 switch-table svc command

Field	Description
Number	Route sequence number in the switching table
Destination	Destination X.121 address
Substitute-src	X.121 source address after substitution; if the content is blank, it means no substitution.
Substitute-dst	X.121 destination address after substitution; if the content is blank, it means no substitution.
CUD	Call User Data
SwitchTo	Forwarding address of this route, which can be an interface, XOT channel or hunt group

display x25 vc

Syntax **display x25 vc** [*lci*]

View Any view

Parameter *lci*: Logical channel identifier in the range 1 to 4095. If not specified, all VCs will be displayed.

Description Use the **display x25 vc** command to display X.25 virtual circuit information.

Note that if no logical channel identifier is specified, the information about all virtual circuits is displayed.

There are three types of virtual circuits as follows:

- An SVC (switched virtual circuit) is set up temporarily by X.25 through calling as required.
- A PVC is configured manually and exists regardless of the data transmission requirement.
- When the device works in X.25 switching mode, virtual circuits will be set up in order to transfer data.

Information about the three types of virtual circuits can be shown with this command, and only some fields of their outputs differ.

Example # Display X.25 VC information.

```
<Sysname> display x25 vc
Interface: Serial2/0
  SVC 1
    State: P4(transmit)
    Map: ip 10.1.1.2 to 130
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 5  Local PR: 5  Remote PS: 5  Remote PR: 4
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 5/5  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 420/420
    Send Queue(Current/Max): 0/200
Interface: Serial2/1/0
  SVC 10
    State: P4(transmit)
    SVC <--> Serial2/0 SVC 60
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 5/5  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 420/420
    Send Queue(Current/Max): 0/200
Interface: Serial2/0-1.1.1.1
  PVC 1
    State: P/Inactive
    XOT PVC <--> Serial2/0 PVC 1 connected
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 0/0  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 0/0
```

```
    Send Queue(Current/Max): 1/200
Interface: Serial2/0
  PVC 1
    State: D3(DCE  reset indication)
    PVC <--> XOT Serial2/0-1.1.1.1 PVC 1 connected
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 0  Local PR: 0  Remote PS: 0  Remote PR: 0
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 0/0  INTERRUPT 0/0
      RR 0/0  RNR 0/0  REJ 0/0
      Bytes 0/0
    Send Queue(Current/Max): 0/200
Interface: Serial2/0
  SVC 59
    State: P4(transmit)
    PAD: UI-130 From remote 130 connected to local 220
    Window size: input 2  output 2
    Packet Size: input 128  output 128
    Local PS: 3  Local PR: 1  Remote PS: 1  Remote PR: 2
    Local Busy: FALSE  Reset times: 0
    Input/Output:
      DATA 9/11  INTERRUPT 0/0
      RR 6/2  RNR 0/0  REJ 0/0
      Bytes 53/363
    Send Queue(Current/Max): 0/200
```

Table 62 Description on the fields of the display x25 vc command

Field	Description
Interface: Serial2/0	Interface name
SVC 1	SVC number
State: P4(transmit)	SVC state: P4 (transmission state)
Map: ip 10.1.1.2 to 130	Address mapping
XOT PVC <--> Serial2/0 PVC 1 connected	PVC from XOT to serial2/0 already established
PVC <--> XOT Serial2/0-1.1.1.1 PVC 1 connected	PVC from serial2/0 to XOT already established
PAD: UI-130 From remote 130 connected to local 220	PAD: User interface index 130, connection from remote X.121 address 130 to local X.121 address 220
Window size: input 2 output 2	VC window size: input 2 output 2
Packet Size: input 128 output 128	Packet Size: input 128 output 128
Local PS: 5 Local PR: 5 Remote PS: 5 Remote PR: 4	Local packet sending sequence number, local packet receiving sequence number, remote packet sending sequence number, remote packet receiving sequence number
Local Busy: FALSE Reset times: 0	Local busy/reset times
Input/Output: DATA 5/5 INTERRUPT 0/0 RR 6/2 RNR 0/0 REJ 0/0 Bytes 420/420	Input/Output : Data 5/5 Break 0/0 Ready to receive 6/2 Not ready to receive 0/0 Reject 0/0 Total bytes of the upper layer 420/420
Send Queue(Current/Max): 0/200	Length of sending queue (current/maximum)

display x25 x2t switch-table

Syntax **display x25 x2t switch-table**

View Any view

Parameter None

Description Use the **display x25 x2t switch-table** command to display the X2T (X.25 to TCP) switching table.

The entry exists when the router sets up an XOT connection and is deleted after the connection is closed.

Example # Display the X2T switching table on the router.

```
<Sysname> display x25 x2t switch-table
    X.121       Interface    [LCD       ] <--> Ip Address  port   SocketId
    ========================================================================
    222         Serial1/0    [SVC:1024  ] <--> 20.1.1.1    102    2
    NULL        Serial1/0    [PVC:1     ] <--> 20.1.1.1    104    2
```

Table 63 Description on the fields of the display x25 x2t switch-table command

Field	Description
X.121	X.121 address
Interface	Interface name
LCD	SVC or PVC connection
Ip Address	IP address
Port	TCP port number
SocketId	Socket ID

display x25 xot

Syntax **display x25 xot**

View Any view

Parameter None

Description Use the **display x25 xot** command to display XOT (X.25 over TCP) connection information, such as peer IP and port, local IP and port, keepalive setting of socket and incoming/outgoing interface names.

Related command: **x25 switch svc xot**, **x25 xot pvc**.

Example # Display XOT connection information.

```
<Sysname> display x25 xot
SVC 1024:  ( ESTAB )
```

```
tcp peer ip: 10.1.1.1, peer port: 1998
tcp local ip: 10.1.1.2, local port: 1024
socket keepalive period: 5, keepalive tries: 3
come interface name: Serial1/0-10.1.1.1-1024
go interface name: Serial1/0
```

lapb max-frame

Syntax **lapb max-frame** *n1-value*

undo lapb max-frame

View Interface view

Parameter *n1-value*: N1 value of the LAPB parameter in bits, in the range 1096 to 12104. It is the maximum value of a frame expected from the DTE or DCE, 8 times the value of MTU plus the protocol header.

Description Use the **lapb max-frame** command to configure the LAPB N1 parameter.

Use the **undo lapb max-frame** command to restore the default.

The default value of N1 is calculated according to the MTU, upper layer protocol and modulo, as shows below:

Table 64 Difference between N1 and MTU (in bytes) versus upper layer protocol and modulo

Upper layer protocol	Modulo	Difference between N1 and MTU (bytes)
IP/IPX	8	4
IP/IPX	128	5
Multiprotocol	8	6
Multiprotocol	128	7
X.25	8	7
X.25	128	8

The default value of N1 varies with MTU and modulo.

For example, upon system initialization, the upper layer protocol is IP, modulo 8 and MTU 1500, so the default value of N1 is (1500+4)*8 = 12032. If the modulo is set to 128, then the default value of N1 is (1500+5)*8 = 12040. You can use the **undo lapb max-frame** command to restore the new default. For the same reason, N1 changes with the change of MTU.

Example # Set the LAPB N1 parameter to 1160 on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] lapb max-frame 1160
```

lapb modulo

Syntax **lapb modulo** { **8** | **128** }

undo lapb modulo

View Interface view

Parameter **8**: Modulo 8.

128: Modulo 128.

Description Use the **lapb modulo** command to specify the LAPB modulo.

Use the **undo lapb modulo** command to restore the default.

The default is modulo 8.

There are two LAPB frame numbering modes: modulo 8 and modulo 128. Each frame (I frame) is numbered in sequence, in the range 0 to the modulo minus 1. Sequence numbers will cycle within the range.

Modulo 8 is the basic mode. It is sufficient for most links.

Related command: **lapb window-size**.

Example # Set the LAPB frame numbering mode on Serial2/0 to modulo 8.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] lapb modulo 8
```

lapb retry

Syntax **lapb retry** *n2-value*

undo lapb retry

View Interface view

Parameter *n2-value*: Value of LAPB N2, indicating the maximum retries that a DCE or DTE sends one frame to DTE or DCE. The value ranges from 1 to 255.

Description Use the **lapb retry** command to configure LAPB parameter N2.

Use the **undo lapb retry** command to restore the default.

The default is 10.

Example # Set the LAPB parameter N2 on Serial 2/0 to 20.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] lapb retry 20
```

lapb timer

Syntax **lapb timer** { **t1** *t1-value* | **t2** *t1-value* | **t3** *t3-value* }

undo lapb timer { **t1** | **t2** | **t3** }

View Interface view

Parameter **t1** *t1-value*: Value of timer T1, in the range 2 to 64000 milliseconds. The default is 3000 milliseconds.

t2 *t2-value*: Value of the timer T2, in the range 1 to 32000 milliseconds. The default is 1500 milliseconds.

t3 *t3-value*: Value of the timer T3, in the range 0 to 255 seconds. The default is 0 seconds.

Description Use the **lapb timer** command to configure the LAPB timers T1, T2 and T3.

Use the **undo lapb timer** command to restore their default values.

T1 is the retransmission timer. When T1 expires, DTE (DCE) will start retransmission. The value of T1 shall be greater than the maximum time between the sending of a frame and the receiving of its response frame.

T2 is the reception timer. When it expires, the DTE/DCE must send an acknowledgement frame so that this frame can be received before the peer DTE/DCE T1 timer expires (T1Š2*T2).

T3 is an idle channel timer, when it expires, the DCE reports to the packet layer that the channel stays idle for a long time. T3 should be greater than the timer T1 (T3>T1) on a DCE. When T3 is 0, it indicates that it does not function yet.

Example # Set the LAPB timer T1 on Serial2/0 to 2000 milliseconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] lapb timer t1 2000
```

lapb window-size

Syntax **lapb window-size** *k-value*

undo lapb window-size

View Interface view

Parameter *k-value*: Maximum number of sequence numbered frames to be acknowledged by DTE or DCE during any specified time. If the modulo is 8, the value of the window parameter K ranges 1 to 7. If the modulo is 128, the value of the window parameter K ranges 1 to 127.

Description Use the **lapb window-size** command to configure the LAPB window parameter K.

Use the **undo lapb window-size** command to restore the default.

The default is 7.

Related command: **lapb modulo**.

Example # Set the LAPB window parameter K on the interface Serial 2/0 to 5.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] lapb window-size 5
```

link-protocol lapb

Syntax **link-protocol lapb** [**dce** | **dte**] [**ip** | **multi-protocol**]

View Interface view

Parameter **dce**: Specifies DCE mode of LAPB.

dte: Specifies DTE mode of LAPB.

ip: Specifies the upper layer protocol as IP.

multi-protocol: Specifies the upper layer protocol as multi-protocol.

Description Use the **link-protocol lapb** command to specify the link layer protocol of the interface as LAPB.

By default, the link layer protocol of an interface is PPP.

When the link layer protocol is LAPB, the default operating mode is DTE, and the upper layer protocol is IP.

Though LAPB is a layer-2 protocol of X.25, it can act as an independent link-layer protocol for simple data transmission. Generally, LAPB can be used when two routers are directly connected with a dedicated line. At that time one end works in the DTE mode, and the other in the DCE mode.

Example # Configure the link layer protocol and operating mode of Serial 2/0 as LAPB and DCE.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol lapb dce
```

link-protocol x25

Syntax **link-protocol x25** [**dce** |**dte**] [**ietf** | **nonstandard**]

View Interface view

Parameter **dce**: Specifies the DCE mode.

dte: Specifies the DTE mode.

Ietf: Encapsulates IP or other network protocols on the X.25 network based on the standard stipulation of the IETF RFC 1356.

nonstandard: Nonstandard encapsulates IP or other network protocols on the X.25 network.

Description Use the **link-protocol x25** command to encapsulate X.25 protocol on the specified interface.

By default, the link-layer protocol for the interface is PPP. When the interface uses X.25 protocol, it works in DTE IETF mode by default.

Note that:

When two Routers are connected via the X.25 public packet network, they shall work as DTE and use IETF format.

If two Routers are directly connected, one Router shall work as DTE, the other as DCE. Both parties should use the same data format.

If the X.25 switching function is used, the device should work as DCE.

In practice, select the IETF format if there is no special requirement.

Example # Specify X.25 as the link layer protocol of the interface Serial2/0 that works in DTE IETF mode.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25 dte ietf
```

pad

Syntax **pad** *x121-address*

View User view

Parameter *x121-address*: Destination X.121 address, a string of 1 to 15 numerical characters.

Description Use the **pad** command to establish a X.25 PAD connection and logon to the remote site.

PAD is similar to telnet. It can establish the connection from the local to the remote through the remote X121 address to carry out configuration operations.

Example # Establish a PAD connection to the destination X.121 address 2.

```
<Sysname> pad 2
```

reset xot

Syntax **reset xot local** *local-ip-address local-port* **remote** *remote-ip-address remote-port*

View User view

Parameter *local-ip-address*: Local IP address of the XOT connection.

local-port: Local port number of the XOT connection.

remote-ip-address: Remote IP address of the XOT connection.

remote-port: Remote port number of the XOT connection.

Description For SVC, use the **reset xot** command to clear an XOT link.

For PVC, use the **reset xot** command to reset an XOT link.

When you clear or reset the XOT link, you can obtain the required ports using the **display x25 xot** or **display tcp status** command.

Example # Clear or reset the XOT link.

```
<Sysname> reset xot local 10.1.1.1 1998 remote 10.1.1.2 1024
```

reset x25

Syntax **reset x25** { **counters interface** *interface-type interface-number* | **vc interface** *interface-type interface-number* [*vc-number*] }

View User view

Parameter **counters**: Resets interface statistics.

vc: Resets X.25 virtual circuit.

interface-type interface-number: Specifies an interface by its type and number.

vc-number: Virtual circuit number of PVC or SVC, in the range 1 to 4095.

Description Use the **reset x25** command to reset X.25 protocol statistics or X.25 virtual circuit on the specified interface.

For PVC number, the command resets the PVC.

For SVC number, the command deletes the SVC.

Example # Reset the X.25 statistics on Serial 2/0.

```
<Sysname> reset x25 counters interface serial 2/0
```

reset lapb statistics

Syntax **reset lapb statistics**

View Interface view

Parameter None

Description Use the **reset lapb statistics** command to clear LAPB statistics.

Example # Clear the LAPB statistics on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] reset lapb statistics
```

translate ip

Syntax **translate ip** *ip-address* **port** *port-number* { **pvc** *interface-type interface-number pvc-number* | **x25** *x.121-address* }

undo translate ip *ip-address* **port** *port-number*

View System view

Parameter *ip-address*: Local IP address.

port *port-number*: TCP port number on which the local router listen messages, in the range 1 to 65535.

Interface-type interface-number: Specifies an interface by its type and number.

pvc-number: PVC number, in the range 1 to 4095.

x.121-address: X.121 address.

Description Use the **translate ip** command to configure an X2T forwarding route from IP network to X.25 network.

Use the **undo translate ip** command to remove the route.

When a host in the IP network sends packets to the specified IP address and port number of the device, the device will translate these IP packets to X.25 ones and then forward them to the specified X.121 address or PVC in the X.25 network.

CAUTION:

- *The maximum number of IP-to-X.25 mappings varies by device.*
- *For the **translate ip** command, if an IP address uses only one port number, port number 102 is preferred whenever possible. If an IP address uses multiple port numbers, port numbers between 1024 and 5000 are recommended and the well-known port numbers (such as 21, 23) are not used to avoid network failure.*

Example # Configure an X2T forwarding route to forward the packets that the local device receives at 10.1.1.1:102 to the X.121 address 111.

```
<Sysname> system-view
[Sysname] translate ip 10.1.1.1 port 102 x25 111
```

Configure an X2T forwarding route to forward the packets that the local device receives at 10.1.1.1:102 to PVC 1 on the interface Serial2/0.

```
<Sysname> system-view
[Sysname] translate ip 10.1.1.1 port 102 pvc serial 2/0 1
```

translate x25

Syntax **translate x25** *x.121-address* **ip** *ip-address* **port** *port-number*

undo translate x25 *x.121-address*

View System view

Parameter *x.121-address:* X.121 address.

ip *ip-address:* IP address of the remote host.

port *port-number*: Port number of the remote host.

Description Use the **translate x25** command to configure an X2T forwarding route from X.25 network to IP network.

Use the **undo translate x25** command to cancel this configuration.

You can implement the packet forwarding from an X.25 network to an IP network using this command. The device compares the destination address in the X.25 call request packet to the *x.121-address*, if they match, then initiates a TCP connection

to the specified IP address and port number. Packets received from the X.25 model are added with an X2T header to forward through the TCP connection.

You can establish mappings between port numbers and X.121 addresses by multiple commands.

CAUTION: *The maximum number of IP-to-X.25 mappings varies by device.*

Example # Configure an X2T forwarding route to forward the packets that are received at the X.121 address 111 to the IP address 10.1.1.1:102.

```
<Sysname> system-view
[Sysname] translate x25 1111 ip 10.1.1.1 port 102
```

x25 alias-policy

Syntax **x25 alias-policy** *match-type alias-string*

undo x25 alias-policy *match-type alias-string*

View Interface view

Parameter *match-type*: Match type of the alias. There are 9 optional match types:

- **free**: Free match
- **free-ext**: Extended free match
- **left**: Left alignment match
- **left-ext**: Extended left alignment match
- **right**: Right alignment match
- **right-ext**: Extended right alignment match
- **strict**: Strict match
- **whole**: Whole match
- **whole-ext**: Extended whole match

alias-string: Alias name, a string of 1 to 17 characters.

Description Use the **x25 alias-policy** command to configure the alias of an X.121 address.

Use the **undo x25 alias-policy** command to delete the alias of an X.121 address.

By default, no x.25 alias is configured.

When an X.25 call is forwarded between networks, different X.25 networks may perform some operations on the destination addresses (that is, the called DTE address) carried by this call packet, for example, regularly adding or deleting the prefix and suffix. In this case, you need to set an interface alias for the router to

adapt this change. Please consult your ISP to learn if the network supports this function before deciding on whether the alias function is enabled or not.

For information about x.25 alias, refer to "x25 alias-policy" on page 441.

Example # Configure the link-layer protocol on interface Serial2/0 as X.25 and its X.121 address to 20112451, and set two aliases with different match types for it.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25
[Sysname-Serial2/0] x25 x121-address 20112451
[Sysname-Serial2/0] x25 alias-policy right 20112451$
[Sysname-Serial2/0] x25 alias-policy left $20112451
```

With the above configurations, a call whose destination address is 20112451 can be accepted as long as it can reach the local X.25 interface Serial2/0, no matter whether the network is performing the prefix adding operation or suffix adding operation.

x25 call-facility

Syntax **x25 call-facility** *facility-option*

undo x25 call-facility *facility-option*

View Interface view

Parameter *facility-option*: User facility option, including:

Table 65 Description on the user facility option

Option	Description
closed-user-group *group number*	Specifies a closed user group (CUG) number for the X.25 interface. The facility enables DTE to belong to one or more CUGs. CUG allows the DTEs in it to communicate with each other, but not to communicate with other DTEs. The group number is in the range 0 to 9999.
packet-size *input-size output-size*	Carries out maximum packet size negotiation in initiating call from the X.25 interface. Maximum packet size negotiation is part of flow control parameter negotiation. It needs two parameters: maximum input packet size and maximum output packet size, which must range from 16 (inclusive) to 4096 (inclusive), and must be the integer power of 2.
reverse-charge-request	Carries reverse charging request when initiating calls from the X.25 interface.
roa-list *roa name*	Specifies an ROA list name for the X.25 interface. The *roa name* is a string of 1 to 19 characters.
send-delay *delay-time*	Carries out the maximum network send delay negotiation when initiating calls from the X.25 interface. The delay time is in the range 0 to 65534 ms.
threshold *input-value output-value*	Specifies throughput negotiation values for initiating calls from the X.25 interface. The values of *input/output* can only be 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, and 48000.

Table 65 Description on the user facility option

Option	Description
window-size *input-window-size output-window-size*	Carries out the window size negotiation when initiating calls from the X.25 interface. Window size negotiation is a part of flow control parameter negotiation. It needs two parameters: input window size and output window size. When the modulo is 8, the size is in the range 1 to 7; when the modulo is 128, it is in the range 1 to 127.

Description Use the **x25 call-facility** command to set user options for an X.25 interface. After an option is set, all X.25 calls from the X.25 interface will carry the relevant information field in call packet.

Use the **undo x25 call-facility** command to delete the set option.

By default, no facility is set.

The user facilities set via this command are available for all the calls originating from this X.25 interface. You can also use the optional parameter *option* of the **x25 map** command to set user facility option for the X.25 call originating from a specific address map. What's more, the priority of user facility configured with the **x25 map** command is higher than that configured with the **x25 call-facility** command.

Related command: **x25 map**, **x25 modulo**.

Example # Specify the flow control parameter negotiation with the peer end for the calls from the X.25 interface serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 call-facility packet-size 512 512
[Sysname-Serial2/0] x25 call-facility window-size 5 5
```

x25 cug-service

Syntax **x25 cug-service** [**incoming-access** | **outgoing-access** | **suppress** { **all** | **preferential** }] *

undo x25 cug-service

View Interface view

Parameter **incoming-access**: Incoming access policy.

outgoing-access: Outgoing access policy.

suppress all: Suppresses all. If the incoming packet contains CUG facility, delete the CUG facility and process the call. It does not apply to outgoing call.

suppress preferential: Processes only the calls configured with preference rule.

Description Use the **x25 cug-service** command to enable CUG service and suppression policies.

Use the **undo x25 cug-service** command to disable CUG service.

By default, CUG service is disabled.

After CUG service is enabled, the system suppresses those calls matching the preset conditions. The details are:

- If no parameter is configured, allow incoming/outgoing calls without CUG facilities, and allow incoming/outgoing calls with CUG facilities after deleting the CUG facilities.
- If the **incoming-access** parameter is chosen, the system suppresses incoming calls. That is, it suppresses the incoming calls that has CUG facilities but has no CUG mapping rules allowing them to pass, and lets the incoming calls without CUG facilities pass through.
- If the **outgoing-access** parameter is chosen, the system suppresses outgoing calls. That is, it suppresses the outgoing calls that has CUG facilities but has no CUG mapping rules allowing them to pass, and lets the outgoing calls without CUG facilities pass through.
- If the **suppress all** parameter is chosen, the system removes CUG facilities for the incoming calls with CUG facilities and makes call processing. This parameter is ineffective to outgoing calls.
- When the **suppress preferential** parameter is included, if an incoming call with CUG facilities and the suppression rule is **preferential**, the system then removes its CUG facilities and make call processing. If the suppression rule is not **preferential**, the system does not remove its CUG facilities but lets it pass through. This parameter is ineffective to outgoing calls.

Related command: **x25 local-cug**.

*The command is used at DCE end. You can use the **link-protocol x25** dce command to set the interface to work in DCE mode.*

Example # Enable CUG service with incoming access policy on the interface Serial2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 cug-service incoming-access
```

x25 default-protocol

Syntax **x25 default-protocol** *protocol-type*

undo x25 default-protocol

View Interface view

Parameter *protocol-type*: Protocol type. IP is available at present.

Description Use the **x25 default-protocol** command to set the default upper-layer protocol of X.25 for the X.25 interface.

Use the **undo x25 default-protocol** command to restore the default.

By default, no upper-layer protocol is specified.

During X.25 SVC setup, the called device will check the call user data field of X.25 call request packet. If it is an unidentifiable one, the called device will deny the setup of the call connection. However, a user can specify a default upper-layer protocol carried over X.25. When X.25 receives a call with unknown CUD, the call can be treated based on the default upper-layer protocol specified by a user.

Example # Set the default upper-layer protocol over the X.25 interface Serial2/0 to IP.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 default-protocol ip
```

x25 hunt-group

Syntax **x25 hunt-group** *hunt-group-name* { **round-robin** | **vc-number** }

undo x25 hunt-group *hunt-group-name*

View System view

Parameter *hunt-group-name*: Name of a hunt group, a string of 1 to 30 characters.

round-robin: Selects call channel using cyclic selection policy.

vc-number: Selects call channel using the policy of computing available logical channel.

Description Use the **x25 hunt-group** command to create or enter an X.25 hunt group.

Use the **undo x25 hunt-group** command to delete the specified X.25 hunt group.

X.25 hunt group supports two call channel selection policies: **round-robin** mode and **vc-number** mode, and a hunt group only uses one channel selection policy. The **round-robin** mode will select next interface or XOT channel inside hunt group for each call request using cyclic selection method. The **vc-number** mode will select the interface with the most idle-logical channels in hunt group for each call request.

A hunt group can have 10 interfaces or XOT channels at most, and it can select the available channels between interface and XOT channel.

XOT channel cannot join the hunt group that adopts the **vc-number** selection policy.

Example # Create hunt group hg1 which uses cyclic selection policy.

```
<Sysname> system-view
[Sysname] x25 hunt-group hg1 round-robin
[Sysname-hg-hg1]
```

x25 ignore called-address

Syntax **x25 ignore called-address**

undo x25 ignore called-address

View Interface view

Parameter None

Description Use the **x25 ignore called-address** command to enable it to ignore the X.121 address of the called DTE when X.25 initiates calls.

Use the **undo x25 ignore called-address** command to disable this function.

By default, this function is disabled.

According to X.25, the calling request packet must carry the address. However, on some occasions, the X.25 calling request does not have to carry the called/calling DTE address in a specific network environment or as is required by the application. This command enables users to specify whether the call request packet sent by X.25 in the device carries the called DTE address.

Related command: **x25 response called-address**, **x25 response calling-address**, **x25 ignore calling-address**.

Example # Specify the call request packet from the X.25 interface Serial 2/0 not to carry the called DTE address.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 ignore called-address
```

x25 ignore calling-address

Syntax **x25 ignore calling-address**

undo x25 ignore calling-address

View Interface view

Parameter None

Description Use the **x25 ignore calling-address** command to enable it to ignore the X.121 address of the calling DTE when X.25 initiates calls.

Use the **undo x25 ignore calling-address** command to disable this function.

By default, this function is disabled.

According to X.25, the calling request packet must carry the address. However, on some occasions, the X.25 calling request does not have to carry the called/calling DTE address in a specific network environment or as is required by the application. This command enables users to specify whether the call request packet sent by X.25 in the device carries the calling DTE address.

Related command: **x25 response called-address**, **x25 response calling-address**, **x25 ignore called-address**.

Example # Specify the call request packet from the X.25 interface Serial 2/0 not to carry the calling DTE address.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 ignore calling-address
```

x25 local-cug

Syntax **x25 local-cug** *local-cug-number* **network-cug** *network-cug-number* [**no-incoming** | **no-outgoing** | **preferential**]*

undo x25 local-cug *cug-number*

View Interface view

Parameter *local-cug-number*: Number of local cug.

network-cug-number: Number of network cug.

no-incoming: Suppresses incoming calls.

no-outgoing: Suppresses outgoing calls.

preferential: Specifies the preference rule.

Description Use the **x25 local-cug** command to configure mapping from local CUG to network CUG and define its suppression rule.

Use the **undo x25 local-cug** command to remove the mapping from local CUG to network CUG.

The command is disabled by default.

CUG map is the exchange relationship between local (DTE device) and network (X.25 network) CUG numbers when the device is processing CUG calls. For

example, if the DTE with CUG number as 10 wants to call the DTE with CUG number as 20 in the network, the device will first find the map in the map table. If the map is found, change the CUG number of the calling packet to 20 and forward the packet; if not found, refuse to forward the packet.

You can specify the suppress rule while configuring CUG map. There are three suppress rules:

1. Suppress income access **no-incoming**
2. Suppress outgoing access **no-outgoing**
3. Specify the preference rule **preferential**

Among them, preference rule is specified as related with suppress CUG policy, that is, if suppress policy is set to suppress CUG in the preferential mapping call (the **suppress preferential** parameter), then delete the CUG facility in the incoming packets of the map and process the calls.

Related command: **x25 call-facility**, **x25 cug-service**.

*If the command is used at DCE side, use the **link-protocol x25** dce command to set the interface as DCE.*

Example # Define the rule on the serial interface Serial2/0: the incoming calls with 100 local CUGs or 200 network CUGs are denied.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 cug-service
[Sysname-Serial2/0] x25 local-cug 100 network-cug 200 no-incoming
```

x25 map

Syntax **x25 map** *protocol-type protocol-address* **x121-address** *x.121-address* [*option*]

undo x25 map { **ip** | **compressedtcp** } *protocol-address*

View Interface view

Parameter *protocol-type*: Protocol type, with **ip** (IP protocol) and/or **compressedtcp** (IP protocol supporting TCP header compression). If you want to configure both of them, ensure that the *protocol-address* are same for both **ip** and **compressedtcp**. The **compressedtcp** requires correct configuration for all the link ends, otherwise, the link may be blocked.

protocol-address: Network protocol address of the peer host.

x121-address *x.121-address*: X.121 address of the peer host.

option: Specifies some attributes or user facilities for the address mapping.

The following gives the detailed information of options:

Table 66 Description on the attributes or user facilities of X.25 address mapping

Option	Description
broadcast	Sends broadcasts of network protocol and multicasts of IP to the destination. This option provides support for some routing protocols (such as Routing Information Protocol).
closed-user-group *group number*	Specifies a closed user group (CUG) number for the X.25 interface, in the range 0 to 9999.
compress	Compresses X.25 payloads.
encapsulation-type	Encapsulation type, with **nonstandard**, **ietf**, **multi-protocol** and **snap** available.
idle-timer *minutes*	Maximum idle time for the VC associated with the address mapping. 0 means that the idle time is infinite.
no-callin	Disables accepting calls to the address mapping.
no-callout	Disables calls originating from the address mapping.
packet-size *input-size output-size*	Carries out maximum packet size negotiation when initiating calls from the mapping. It needs two parameters: maximum input packet size and maximum output packet size, which must range from 16 to 4096 bytes, and must be the integer power of 2.
reverse-charge-accept	If a call initiated by the address mapping carries reverse charging request, to accept the call, this option must be configured in the address mapping.
reverse-charge-request	Specifies calls from the address mapping to carry reverse charging requests
roa-list *roa-name*	Specifies an ROA list name for the X.25 interface. The *roa name* is a string of 1 to 19 characters.
send-delay *delay-time*	Carries out the maximum network transmission delay negotiation when initiating calls from the mapping. The delay time is in the range 0 to 65534 ms.
threshold *input-value output-value*	Specifies threshold values when initiating throughput negotiation with the peer from the mapping. The values of *input/output* can only be 75, 150, 300, 600, 1200, 2400, 4800, 9600, 19200, or 48000.
vc-per-map *count*	Maximum number of VCs associated with the address mapping, in the range 1 to 8.
window-size *input-window-size output-window-size*	Carries out the window size negotiation with the peer when initiating calls from the address mapping, including input window size and output window size. When the modulo is 8, the size is in the range 1 to 7; when the modulo is 128, it is in the range 1 to 127.

Description

Use the **x25 map** command to set the address mapping between IP address and X.121 address.

Use the **undo x25 map** command to delete a mapping.

By default, no address mapping is configured.

Since X.25 protocol can multiplex multiple logical virtual circuits on a physical interface, you need to manually specify the mapping relation between all network addresses and X.121 addresses.

Once you have specified an address mapping, its contents (including protocol address, X.121 address and all options) cannot be changed. To make

modifications, you can first delete this address mapping via the **undo x25 map** command, and then establish one new address mapping.

Two or more address mappings with an identical protocol address shall not exist on the same X.25 interface.

Related command: **display x25 map**, **x25 reverse-charge-accept**, **x25 call-facility**, **x25 timer idle**, **x25 vc-per-map**.

Example # Set two address mappings on the X.25 interfaces Serial2/1 and Serial2/0, respectively, and the four address mappings have different attributes.

```
<Sysname> system-view
[Sysname] interface serial 2/1
[Sysname-Serial2/1] x25 map ip 202.38.160.11 x121-address 20112451 reverse-c
harge-request reverse-charge-accept
[Sysname-Serial2/1] x25 map ip 202.38.160.138 x121-address 20112450 packet-s
ize 512 512 idle-timer 10
[Sysname-Serial1/0] quit
[Sysname] interface serial2/0
[Sysname-Serial2/0] x25 map ip 20.30.4.1 x121-address 25112451 window-size 4
 4 broadcast
[Sysname-Serial2/0] x25 map ip 20.30.4.8 x121-address 25112450 no-callin
```

x25 modulo

Syntax **x25 modulo** { **8** | **128** }

undo x25 modulo

View Interface view

Parameter **8**: Uses modulo 8 mode.

128: Uses modulo 128 mode.

Description Use the **x25 modulo** command to set the modulo mode of the X.25 interface.

Use the **undo x25 modulo** command to restore the default.

The default is modulo 8 mode.

The slip window is the basis for X.25 traffic control, and the key about the slip window is that the sent packets are numbered cyclically in order and are to be acknowledged by the peer end. The order in numbering refers to the ascending order, like "...2, 3, 4, 5, 6..." "Cyclically" means that the numbering starts again from the beginning when a certain number (called modulo) is reached. For example, when the modulo is 8, the numbering goes "...4, 5, 6, 7, 0, 1..."

X.25 defines two numbering modulo: 8 (also called the basic numbering) and 128 (also called extended numbering).

- *The packet numbering mode on the pair of DTE and DCE must be the same*
- *You need to run the **shutdown** and **undo shutdown** commands on the interface to apply the new configuration.*
- *The packet numbering mode of X.25 Layer 3 is different from the frame numbering mode of LAPB (Layer 2 in X.25). When modulo 128 is applied to the DTE/DCE interface with high throughput, it improves only the efficiency of local DTE/DCE interface (point-to-point efficiency) for LAPB; while for Layer 3 in X.25, it improves the efficiency of the two communicating DTE peers (or peer-to-peer efficiency).*

Example # Set the modulo on the X.25 interface Serial 2/0 to 128.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 modulo 128
```

x25 packet-size

Syntax **x25 packet-size** *input-packet output-packet*

undo x25 packet-size

View Interface view

Parameter *input-packet*: Maximum input packet length in bytes, ranging from 16 (inclusive) to 4096 (inclusive) and must be the integer power of 2.

output-packet: Maximum output packet length in bytes, its value ranges from 16 (inclusive) to 4096 (inclusive) and must be the integer power of 2.

Description Use the **x25 packet-size** command to set the maximum input and output packet lengths of X.25 interface.

Use the **undo x25 packet-size** command to restore their default values.

By default, the maximum input packet length is 128 bytes, and the maximum output packet length is 128 bytes.

Normally, an X.25 packet-switching network has a limitation of the transmission packet size, and the maximum size of a data packet sent by the DTE shall not exceed this size (otherwise it will trigger the reset of the VC). In this way, the DTE devices at sending end and receiving end are required to have datagram fragmentation and reassembly functions. The DTE device at sending end fragments the datagram with a length exceeding the maximum transmission packet length based on the maximum transmission packet length, and sets M bit in other fragments except the final fragment. After receiving these fragments, the DTE at receiving end will reassemble them to a datagram and submit it to the upper-layer protocol based on the M bit. Consult access ISP about this maximum receiving packet length.

Normally, the maximum receiving packet length is equivalent to the maximum sending packet. Unless access ISP allows, do not configure these two parameters with different values.

Example # Set the maximum receiving packet length and maximum sending packet length on X.25 interface Serial 2/0 to 256 bytes.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 packet-size 256 256
```

x25 pvc

Syntax **x25 pvc** *pvc-number protocol-type protocol-address* **x121-address** *x.121-address* [*option*]

undo x25 pvc *pvc-number*

View Interface view

Parameter *pvc-number*: PVC number, in the range 1 to 4095 (inclusive), and must be in the PVC channel range.

protocol-type: Upper-layer protocol carried over the permanent virtual circuit, which may be **IP** (indicating that the upper-layer network protocol is IP protocol) or **compressedtcp** (indicating that the upper-layer network protocol is IP protocol, and supports TCP head compressing).

protocol-address: Network protocol address of the peer end of the PVC.

x121-address *x.121-address*: X.121 address of the peer end of this PVC.

option: Attribute option of the PVC. Detailed description of PVC options:

Table 67 Description on PVC attribute option

Option	Description
broadcast	Forwards broadcast packets to the PVC peer.
encapsulation-type	Encapsulation type, which may be **nonstandard**, **ietf**, **multi-protocol** or **snap**.
compress	Compresses X.25 payload.
packet-size *input-packet output-packet*	Specifies the maximum input packet length and maximum output packet length in bytes, which must range from 16 to 4096, and must be the integer power of 2.
window-size *input-window-size output-window-size*	Specifies the input and output window sizes of the PVC. When the modulo is 8, it is in the range 1 to 7; when the modulo is 128, it is in the range 1 to 127.

Description Use the **x25 pvc** command to configure a PVC route.

Use the **undo x25 pvc** command to delete a PVC route.

By default, no PVC is created. When creating such a PVC, if you do not set the relevant attributes for the PVC, its flow control parameters will be the same as that of the X.25 interface (the flow control parameters on an X.25 interface can be set by the **x25 packet-size** and **x25 window-size** commands).

As one corresponding address mapping is created along with the PVC, it is unnecessary (or impossible) to establish an address mapping first before creating PVCs.

Before creating PVCs, you should first enable the PVC channel range. The range is between 1 and the latest unprohibited channel PVC number minus 1 (including 1 and the lowest PVC number minus 1). Naturally, if the lowest PVC number is 1, the PVC section will be disabled. The following table shows some typical PVC ranges.

Table 68 PVC channel ranges for some typical configurations

PVC channel range	Incoming-only channel range	Two-way channel range	Outgoing-only channel range
Disabled	[0, 0]	[1, 1024]	[0, 0]
[1, 9]	[0, 0]	[10, 24]	[0, 0]
Disabled	[1, 10]	[15, 30]	[0, 0]
[1, 4]	[5, 10]	[15, 25]	[30, 32]
[1, 19]	[0, 0]	[0, 0]	[20, 45]
[1, 4094]	[0, 0]	[0, 0]	[4095, 4095]

Example # Configure the link layer protocol on the interface Serial 2/0 as X.25, enable PVC channel range, and set two PVCs.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25
[Sysname-Serial2/0] x25 vc-range bi-channel 8 1024
[Sysname-Serial2/0] x25 pvc 2 ip 202.38.168.1 x121-address 20112451
broadcast packet-size 512 512
[Sysname-Serial2/0] x25 pvc 6 ip 202.38.168.3 x121-address 20112453
broadcast window-size 5 5
```

x25 queue-length

Syntax **x25 queue-length** *queue-length*

undo x25 queue-length

View Interface view

Parameter *queue-length*: Queue length in packets, ranging from 0 to 9999. The *queue-length* of 0 indicates sending no packets.

Description Use the **x25 queue-length** command to set the data queue length for X.25 VC.

Use the **undo x25 queue-length** command to restore the default.

The default is 200.

When the data traffic is too heavy, you can use this command to extend the receiving queue and sending queue of the X.25 VC to avoid data loss that may affect transmission performance. Note that modifying this parameter would not affect the existing data queue of VC. After changing the parameter, you need to restart the port with the **shutdown**/**undo shutdown** command and this will clear the current SVCs and reset the PVCs, thus change the data queue of all the VCs.

Example # Set the VC data queue length of the X.25 interface Serial 2/0 to 75 packets.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 queue-length 75
```

x25 receive-threshold

Syntax **x25 receive-threshold** *count*

undo x25 receive-threshold

View Interface view

Parameter *count*: Number of packets that can be received before acknowledgement, in the range 0 to input window size. If it is set to 0 or the input window size, this function will be disabled. If it is set to 1, X.25 of the device will send an acknowledgement for each correctly received packet.

Description Use the **x25 receive-threshold** command to set the maximum number of packets that can be received before X.25 sends the acknowledged packet.

Use the **undo x25 receive-threshold** command to restore the default.

The default is 0, that is, the function is disabled.

With this function enabled, the device can send acknowledgement to the peer upon the receipt of some correct packets, even if the input window is not yet full. If data traffic is normal, you may pay more attention to the response speed, and then you can appropriately adjust this parameter to meet the requirement.

Related command: **x25 window-size**.

Example # Specify that each VC on the X.25 interface Serial 2/0 acknowledges each correctly received data packet.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 receive-threshold 1
```

x25 response called-address

Syntax **x25 response called-address**

undo x25 response called-address

View Interface view

Parameter None

Description Use the **x25 response called-address** command to enable X.25 call reception packets to carry the address information of the called DTE.

Use the **undo x25 response called-address** command to disable the above function.

By default, this function is disabled.

According to X.25, the call reception packet may or may not carry an address code group, depending on the specific network requirements. This command enables users to easily specify whether the packet carries the called DTE address.

Related command: **x25 response calling-address**, **x25 ignore called-address**, **x25 ignore calling-address**.

Example # Specify that the call receiving packet of a call sent from the X.25 interface Serial 2/0 carries the called DTE address.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 response called-address
```

x25 response calling-address

Syntax **x25 response calling-address**

undo x25 response calling-address

View Interface view

Parameter None

Description Use the **x25 response calling-address** command to enable X.25 to carry the address information of the calling DTE in call reception packets

Use the **undo x25 response calling-address** command to restore the default.

By default, this function is disabled.

According to X.25, the call reception packet of a call may or may not carry an address code group, depending on the specific network requirements. This command enables users to easily specify whether the call reception packet carries the calling DTE address.

Related command: **x25 response called-address**, **x25 ignore called-address**, **x25 ignore calling-address**.

Example # Specify that the call reception packet of a call sent from the X.25 interface Serial 2/0 carries the calling DTE address.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 response calling-address
```

x25 reverse-charge-accept

Syntax **x25 reverse-charge-accept**

undo x25 reverse-charge-accept

View Interface view

Parameter None

Description Use the **x25 reverse-charge-accept** command to enable this interface to accept the call with the reverse charging request user facility.

Use the **undo x25 reverse-charge-accept** command to disable this function.

By default, this function is disabled.

This function does not affect any call without "reverse charging request".

If you enable this function on an X.25 interface, all these calls that reach the interface will be accepted. If you enable this function for a certain address mapping by the option **reverse-charge-accept** in the **x25 map** command, only such calls that reach the interface and map this address will be accepted, while other calls (carrying reverse charging request and not mapping this address) will be cleared.

Related command: **x25 map**.

Example # Enable Serial 2/0 to accept the call with the reverse charging request user facility.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 reverse-charge-accept
```

x25 roa-list

Syntax **x25 roa-list** *roa-name roa-id*&<1-10>

undo x25 roa-list *roa-name*

View System view

Parameter *roa-name*: Name of ROA, a string of 1 to 19 characters.

roa-id&<1-10>: ROA ID. Its value ranges from 0 to 9999. You can specify 10 IDs for the ROA.

Description Use the **x25 roa-list** command to define ROA list.

Use the **undo x25 roa-list** command to delete ROA list items.

By default, no ROA list is defined.

You can configure multiple (0 to 20. The maximum number of ROA lists supported by the system is 1,000) ROAs. After configuring ROA, you can reference it by its name in the commands **x25 call-facility** or **x25 map**.

Related command: **x25 call-facility**, **x25 map**.

Example # Define two ROA lists, and apply them to the interfaces Serial 2/0 and Serial 2/1 respectively.

```
<Sysname> system-view
[Sysname] x25 roa-list list1 11 23 45
[Sysname] x25 roa-list list2 345
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 call-facility roa-list list1
[Sysname-Serial2/0] quit
[Sysname] interface serial 2/1
[Sysname-Serial2/1] x25 call-facility roa-list list2
```

x25 switch pvc

Syntax **x25 switch pvc** *pvc-number1* **interface** *interface-type interface-number* [**dlci** *dlci-number*] **pvc** *pvc-number2* [*option*]

undo x25 switch pvc *pvc-number1*

View Interface view

Parameter *pvc-number1*: PVC number on the input interface, and its value ranges from 1 to 4095.

interface *interface-type interface-number*: Specifies an interface by its type and number.

dlci *dlci-number*: Specifies an DLCI. The *dlci-number* argument is in the range 16 to 1007.

pvc *pvc-number2*: PVC number on the output interface, and its value ranges from 1 to 4095.

option: Attribute option of PVC.

Description for options:

- **packet-size** *input-packet output-packet*: Specifies the maximum and output packet sizes in bytes, which range from 16 to 4096, and must be the integer power of 2.
- **window-size** *input-window-size output-window-size*: Specifies the input and output window sizes of the VC. When the modulo is 8, it is in the range 1 to 7; when the modulo is 128, it is in the range 1 to 127.

Description Use the **x25 switch pvc** command to configure a PVC route.

Use the **undo x25 switch pvc** command to delete a PVC route.

By default, no PVC route is defined.

Based on the X.25 switching configuration, you can use the device as a simple X.25 switch. When PVC switching is configured, the link layer protocol on the input and output interfaces must be X.25. Moreover, the specified PVCs on the two interfaces are effective. After configuring the PVC switching route, the device will receive information from the PVC of the input interface and forward the information through the specified PVC of the output interface.

You can configure X.25 PVC switching to switch from an X.25 interface to an Annex G DLCI (X.25 over FR) or vice versa, or even between Annex G DLCIs.

Two X.25 networks can be connected via an Annex G DLCI over an FR network. The Annex G DLCI can also act as a backup connection between the two X.25 networks.

You need to configure the switching route for the other interface when configuring switching; otherwise, the switching does not work.

For X.25 PVC switching, you need to specify the VC range first to make it work; otherwise, the PVC switching in the X.25 template cannot work unless you apply a new template to the FR DLCI or delete the current template.

Note that PVC switching cannot be configured on the X.25 sub-interface.

Example # Perform the packet switching from PVC1 on the Serial2/0 to PVC2 on the Serial2/1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 switch pvc 1 interface serial 2/1 pvc 2
```

Perform the packet switching from Annex G DLCI PVC1 on the Serial2/1 to PVC1 on the Serial2/0.

```
<Sysname> system-view
[Sysname] x25 template switch
[Sysname-x25-switch] x25 vc-range bi-channel 10 20
[Sysname-x25-switch] x25 switch pvc 1 interface serial 3/0 pvc 1
[Sysname-x25-switch] quit
[Sysname] interface serial 2/1
[Sysname-Serial2/1] link-protocol fr
[Sysname-Serial2/1] fr interface-type dce
[Sysname-Serial2/1] fr dlci 100
[Sysname-fr-dlci-Serial2/1-100] annexg dce
[Sysname-fr-dlci-Serial2/1-100] x25-template switch
[Sysname-fr-dlci-Serial2/1-100] quit
[Sysname-Serial2/1] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25 dce
[Sysname-Serial2/0] x25 switch pvc 1 interface serial2/1 dlci 100 pvc 1
```

x25 switch svc

Syntax **x25 switch svc** [*-number*] *x.121-address* [**sub-dest** *destination-address*] **sub-source** *source-address*] **interface** *interface-type interface-number* [**dlci** *dlci-number*]

undo x25 switch svc *x.121-address* [**sub-dest** *destination-address*] [**sub-source** *source-address*] [**interface** *interface-type interface-number*]

View System view

Parameter *x.121-address*: Destination X.121 address, a pattern matching string with 1 to 15 numeric characters. For the specific description of mode matching, see the following description. If no wildcard is used, the X.121 address should be exactly matched.

Table 69 X.121 mode matching rules

Wildcard characters	Matching rules	Example	Matchable character string
*	Matching zero or more previous characters	fo*	fo, foo, fooo
+	Matching one or more previous characters	fo+	foo, fooo
^	Matching the beginning of the entered characters	^hell	hell, hello, hellaaa
$	Matching the end of the entered characters	ar$	ar, car, hear
char	Matching a single character specified by char.	s	bs
.	Matching arbitrary single character	l.st	last, lbst, lost

Table 69 X.121 mode matching rules

Wildcard characters	Matching rules	Example	Matchable character string
.*	Matching arbitrary zero or more characters	fo.*	fo, foo, fot
.+	Matching arbitrary one or more characters	fo.+	foo, fot, foot

Table 70 Input rules of X.121 address mode matching string

Characters	Input rules
*	Cannot be placed at the beginning of character string
	Cannot be placed after the symbol ^
	Cannot be placed before and after the symbols + and *.
+	Cannot be placed at the beginning of character string
	Cannot be placed after the symbol ^
	Cannot be placed before and after the symbols + and *.
	Cannot be placed at the end of character string
^	Cannot be placed before the symbols + and *.

-number: SVC route number.

sub-dest *destination-address*: Replaces the destination X.121 address, an alphanumeric string of 1 to 15 characters. The system replaces the destination DTE address in the call request packet with the *destination-address*.

sub-source *source-address*: Replaces the source X.121 address, an alphanumeric string of 1 to 15 characters. The system replaces the source DTE address in the call request packet with the *source-address*.

interface *interface-type interface-number*: Interface type and interface number.

dlci *dlci-number*: Specifies an DLCI. The *dlci-number* argument is in the range 16 to 1007.

Description

Use the **x25 switch svc** command to configure an SVC (switching virtual circuit), indicating the packet to be forwarded to the destination address through the specified interface.

Use the **undo x25 switch svc** command to delete the SVC route.

A device with X.25 switching configured can act as a simple X.25 switch.

The output interface of the SVC switching can be an X.25 interface, or FR interface Annex G DLCI. The link layer of the output interface must be X.25, or FR with the Annex G DLCI configured for output.

Before using this command, you should use the **x25 switching** command to enable X.25 switching.

By default, no SVC is defined.

Example # Configure an SVC to forward the packet to the X.121 address 20112451 through interface Serial2/0.

```
<Sysname> system-view
[Sysname-Serial2/0] x25 switch svc 20112451 interface serial 2/0
```

Configure an SVC to forward the packet to the address 3 through the Annex G DLCI 100 of interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr dlci 100
[Sysname-Serial2/0] annexg dce
[Sysname-Serial2/0] quit
[Sysname] x25 switch svc 3 interface serial 2/0 dlci 100
```

x25 switch svc hunt-group

Syntax **x25 switch svc** *x.121-address* [**sub-dest** *destination-address* | **sub-source** *source-address*] * **hunt-group** *hunt-group-name*

undo x25 switch svc *x.121-address* [**sub-dest** *destination-address*] [**sub-source** *source-address*] [**hunt-group** *hunt-group-nam*e]

View System view

Parameter *x.121-address*: Destination X.121 address, a pattern matching string with 1 to 15 numeric characters. For the specific description of pattern matching, see Table 69 and Table 70. If no wildcard is used, the X.121 address is must be exactly matched.

sub-dest *destination-address*: X.121 address, an alphanumeric string of 1 to 15 characters. The system replaces the destination DTE address in the call request packet with the *destination-address*.

sub-source *source-address*: X.121 address, an alphanumeric string of 1 to 15 characters. The system replaces the source DTE address in the call request packet with the *source-address*.

hunt-group *hunt-group-name*: Specifies a hunt group.

Description Use the **x25 switch svc hunt-group** command to add an X.25 switching SVC whose forwarding address is a hunt group.

Use the **undo x25 switch svc hunt-group** command to delete the specified X.25 switching SVC.

By default, no X.25 switching SVC is configured.

Note that:

- After the X.25 switching SVC with forwarding address being a hunt group is configured, the relevant X.25 call request packet will be forwarded to different

interfaces or XOT channels in the specified hunt group, to implement the load sharing of X.25 protocol.

- X.25 hunt group supports source address and destination address replacement. With destination address replacement, you can hide X.121 address of DTE inside the hunt group so that the outside DTE knows only the X.121 address of the hunt group, therefore enhancing network security inside the hunt group. With source address replacement, you can hide X.121 address of DTE outside the hunt group so that the inside DTE knows only the source X.121 address after replacement but not the source X.121 address the call connects, therefore protecting you privacy.

Related command: **display x25 switch-table svc**.

Example # Add an X.25 switching SVC, whose destination X.121 address is 111 and forwarding address is the hunt group hg1, and substitute the destination address with 9999 and the source address with 8888.

```
<Sysname> system-view
[Sysname] x25 switch svc 111 sub-dest 9999 sub-source 8888 hunt-group hg1
```

x25 switch svc xot

Syntax **x25 switch svc** *x.121-address* [**sub-dest** *destination-address* | **sub-source** *source-address*] * **xot** *ip-address*&<1-6> [*xot-option*]

undo x25 switch svc *x.121-address* [**sub-dest** *destination-address*] [**sub-source** *source-address*] [**xot** *ip-address*&<1-6>]

View System view

Parameter *x.121-address*: Destination address of X.121, a mode matching string with a 1 to 15 numeric characters. For the specific description of mode matching, see Table 69 and Table 70. If no wildcard is used, the X.121 address must exactly match.

sub-dest *destination-address*: X.121 address, a string of 1 to 15 characters. The system replaces the destination DTE address in the call request packet with the *destination-address*.

sub-source *source-address*: X.121 address, a string of 1 to 15 characters. The system replaces the source DTE address in the call request packet with the *source-address*.

xot *ip-address*&<1-6>: Destination IP address of XOT connection, up to 6 addresses can be configured.

xot-option: XOT channel parameter option. For the specific configuration, see Table 71.

Table 71 XOT channel parameter option

Option	Description
timer *seconds*	Keepalive timer delay of XOT connection. The timer sends the keepalive packet upon timeout to detect the connection availability. Its value ranges from 1 to 3600.
retry *times*	Number of maximum retries of sending keepalive. If the number exceeds times, the XOT connection will be disconnected. Its value ranges from 3 to 3600.
source *interface-type interface-number*	Type and number of the interface that initiates the XOT connection.

Description Use the **x25 switch svc xot** command to add an X.25 switching route whose forwarding address is XOT channel.

Use the **undo x25 switch svc xot** command to delete the specified X.25 switching route.

By default, no X.25 switching route is configured.

After configuring the XOT switching command of X.25 SVC, a user can cross IP network from the local X.25 network to implement the interconnection with the remote X.25 network. If a user configures the keepalive attribute, the link detection for XOT will be supported.

Example # Configure a XOT route and forward the packet whose destination X.121 address is 1 to the destination address whose IP address is 10.1.1.1.

```
<Sysname> system-view
[Sysname] x25 switch svc 1 xot 10.1.1.1
```

x25 switching

Syntax **x25 switching**

undo x25 switching

View System view

Parameter None

Description Use the **x25 switching** command to enable the X.25 switching function.

Use the **undo x25 switching** command to disable this function, which will not affect the established VC switching.

By default, X.25 packet switching function is disabled.

X.25 packet switching is used to accept packets from an X.25 interface and send them to a certain interface based on the destination information contained in the packets. The device with this function can be used as a small-sized packet switch.

Example # Enable X.25 switching function.

```
<Sysname> system-view
[Sysname] x25 switching
```

x25 timer hold

Syntax **x25 timer hold** *minutes*

undo x25 timer hold

View Interface view

Parameter *minutes*: Value of delay time in minutes, in the range 0 to 1000.

Description Use the **x25 timer hold** command to set the delay for sending another calling request to a destination to which a previous request failed to reach.

Use the **undo x25 timer hold** command to restore the default.

By default, the delay time is 0 second.

Frequently sending call requests to a wrong destination (which does not exist or is faulty) will deteriorate the operating efficiency of the device. Using this function can avoid this problem to a certain extent. If the previous call failed at one destination, the X.25 would not send calls to such a destination again within the specified time.

If this parameter is set to 0, it is equal to disabling the function. In addition, this function is only effective to the calls originating from the local. That is to say, this parameter is meaningless when the X.25 operates in the switching mode.

Example # Set the delay of the X.25 interface Serial 2/0 to 5 minutes.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 timer hold 5
```

x25 timer idle

Syntax **x25 timer idle** *minutes*

undo x25 timer idle

View Interface view

Parameter *minutes*: Maximum idle time of SVC in minutes, ranging from 0 to 255.

Description Use the **x25 timer idle** command to set the maximum idle time of the SVC on the interface.

Use the **undo x25 timer idle** command to restore the default.

By default, this value is 0.

Note that:

- When a SVC stays idle (no data are transmitted) for a period specified with the **x25 timer idle** command, the router will clear this SVC automatically.
- The **x25 timer idle** command applies to all the SVCs under the interface. You can also use the options in the **x25 map** command to configure the maximum idle time for the SVC related to the address mapping and the priority is higher than the configuration of the interface.
- If the value is set to 0, this SVC will be reserved no matter how long it stays idle.
- Using this command does not work for PVC or the established SVC of X.25 switching.

Related command: **x25 map**.

Example # Set the maximum idle time of the SVC on the interface Serial 2/0 to 10 minutes.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 timer idle 10
```

x25 timer tx0

Syntax **x25 timer tx0** *seconds*

undo x25 timer tx0

View Interface view

Parameter *seconds*: X.25 restart timer in seconds. It ranges 0 to 1000.

Description Use the **x25 timer tx0** command to set the restart timer for DTE (or DCE).

Use the **undo x25 timer tx0** command to restore the default.

The default restart timer on the X.25 DTE is 180 seconds and that on the DCE is 60 seconds.

According to X.25, a timer should be started when the DTE sends a restart request (or a DCE sends a restart indication). If no peer acknowledgement is received after the timer timeout, the sending end will take some measures to guarantee the normal proceeding of the local procedure. This parameter specifies the time of this timer.

Related command: **x25 timer tx1**, **x25 timer tx2**, **x25 timer tx3**.

Example # Set the restart timer on the X.25 interface Serial 2/0 to 120 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 timer tx0 120
```

x25 timer tx1

Syntax **x25 timer tx1** *seconds*

undo x25 timer tx1

View Interface view

Parameter *seconds*: Time of calling request (indication) sending timer in seconds, ranging from 0 to 1000.

Description Use the **x25 timer tx1** command to set calling request (indication) sending timer for the DTE (or DCE).

Use the **undo x25 timer tx1** command to restore the default.

By default, the timer time on a DTE is 200 seconds, and that on a DCE is 180 seconds.

According to X.25, a timer should be started when the DTE sends a call request (or the DCE sends a call indication). If no peer acknowledgement is received after the timer timeout, the sending end will take some measures to guarantee the normal proceeding of the local procedure. This parameter specifies the time of this timer.

Related command: **x25 timer tx0**, **x25 timer tx2**, **x25 timer tx3**.

Example # Set calling request (indication) sending timer on the X.25 interface Serial2/0 to 100 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 timer tx1 100
```

x25 timer tx2

Syntax **x25 timer tx2** *seconds*

undo x25 timer tx2

View Interface view

Parameter *seconds*: Reset request (indication) timer in seconds, ranging from 1 to 1000.

Description Use the **x25 timer tx2** command to set the reset request (indication) timer for DTE (or DCE).

Use the **undo x25 timer tx2** command to restore the default.

By default, the timer on a DTE is 180 seconds, and that on a DCE is 60 seconds.

According to X.25, a timer should be started when a DTE sends a reset request (or a DCE sends a reset indication). If no peer acknowledgement is received after the timer timeout, the sending end will take some measures to guarantee the normal proceeding of the local procedure.

Related command: **x25 timer tx0**, **x25 timer tx1**, **x25 timer tx3**.

Example # Set the reset timer on the X.25 interface Serial1/0 to 120 seconds.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] x25 timer tx2 120
```

x25 timer tx3

Syntax **x25 timer tx3** *seconds*

undo x25 timer tx3

View Interface view

Parameter *seconds*: Time of the clear request (indication) sending timer in seconds, ranging from 1 to 1000.

Description Use the **x25 timer tx3** command to set the clear request (indication) sending timer for DTE (or DCE).

Use the **undo x25 timer tx3** command to restore the default.

By default, the clear timer on a DTE is 180 seconds, and that on a DCE is 60 seconds.

According to X.25, a timer should be started when a DTE sends a clear request (or a DCE sends a clear indication). If no peer acknowledgement is received after the timer timeout, the sending end will take some measures to guarantee the normal proceeding of the local procedure.

Related command: **x25 timer tx0**, **x25 timer tx1**, **x25 timer tx2**.

Example # Set the clear timer on the X.25 interface Serial 2/0 to 100 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 timer tx3 100
```

x25 vc-per-map

Syntax **x25 vc-per-map** *count*

undo x25 vc-per-map

View Interface view

Parameter *count*: Maximum number of VCs, ranging from 1 to 8.

Description Use the **x25 vc-per-map** command to set the maximum number of VCs for connections with the same destination device.

Use the **undo x25 vc-per-map** command to restore the default.

The default is 1.

If the parameter is greater than 1, and the sending window and the sending queue of VC are filled full, the system will create a new VC to the same destination. If the new VC cannot be created, packets will be discarded.

Example # Set the maximum value of VCs on the X.25 interface Serial 2/0 to 3.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 vc-per-map 3
```

x25 vc-range

Syntax **x25 vc-range** { **bi-channel** *ltc htc* [**out-channel** *loc hoc*] | **in-channel** *lic hic* [**bi-channel** *ltc htc*] [**out-channel** *loc hoc*] | **out-channel** *loc hoc* }

undo x25 vc-range

View Interface view

Parameter **bi-channel** *ltc htc*: Lowest and highest two-way channels of X.25 VC, and its value ranges from 0 to 4095. If *htc* (highest two-way channel) is set to 0, *ltc* (lowest two-way channel) must also be set to 0, which indicates that the two-way channel section is disabled.

out-channel *lic hic*: Lowest and highest incoming-only channels of X.25 VC, and its value ranges from 0 to 4095. If *hic* (highest incoming-only channel) is set to 0, *lic* (lowest incoming-only channel) must also be set to 0, which indicates that the incoming-only channel section is disabled.

in-channel *loc hoc*: Lowest and highest outgoing-only channels of X.25 VC, and its value ranges from 0 to 4095. If *hoc* (highest outgoing-only channel) is set to 0, *loc* (lowest outgoing-only channel) must also be set to 0, which indicates that the outgoing-only channel section is disabled.

Description Use the **x25 vc-range** command to set the upper and lower limits of X.25 VC range.

Use the **undo x25 vc-range** command to restore their default values.

By default, the upper and lower limits of two-way channel are 1 and 1024, of incoming-only channel are both 0, and of outgoing-only channel are both 0.

By default, X.25 bans the incoming-only and outgoing-only channel sections and reserves only the double direction channel section (in the range 1 to 1024). Please configure the range correctly according to your ISP's requirement.

Example # Configure the incoming-only, two-way and outgoing-only channel ranges as [1, 7], [8, 1024] and [0, 0] respectively.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 vc-range in-channel 1 7 bi-channel 8 1024
```

x25 window-size

Syntax **x25 window-size** *input-window-size output-window-size*

undo x25 window-size

View Interface view

Parameter *input-window-size*: Size of input window. When X.25 window modulo is 8, its value ranges from 1 to 7. When X.25 window modulo is 128, its value ranges from 1 to 127.

output-window-size: Size of output window. When X.25 window modulo is 8, its value ranges from 1 to 7. When X.25 window modulo is 128, its value ranges from 1 to 127.

Description # Set calling request (indication) sending timer on the X.25 interface Serial2/0 to 100 seconds.

Use the **undo x25 window-size** command to restore their default values.

The default sizes are both 2.

The *input-window-size* determines the maximum number of correctly received packets before X.25 sends the acknowledgement information. As long as the bandwidth allows, the greater the window size, the higher the transmission efficiency.

The parameter *out-window-size* determines the maximum number of data packets sent by X.25 before it receives the correct acknowledgment information. As long as the bandwidth allows, the greater the window size, the higher the transmission efficiency.

Please consult your ISP about the input and output window sizes. Unless supported by the network, do not set these two parameters to different values.

Example # Set the input and output window sizes on the X.25 interface Serial 2/0 to 5.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 window-size 5 5
```

x25 x121-address

Syntax **x25 x121-address** *x.121-address*

undo x25 x121-address

View Interface view

Parameter *x.121-address*: X.121 address, an alphanumeric string of 1 to 15 characters.

Description Use the **x25 x121-address** command to set the X.121 address of an X.25 interface.

Use the **undo x25 x121-address** command to delete the address.

Note that:

- If the device is accessed to X.25 public packet network, the ISP must assign a valid X.121 address to it. If two devices are only directly connected back to back, you can randomly specify the valid X.121 address. If you only want the device to work in switching mode, the X.121 address needs not to be configured.
- When you reconfigure an X.121 address for an X.25 interface, you need not delete the original X.121 address, because the new address will overwrite the old one.

For the format of the X.121 address and the dynamic conversion between IP address and X.121 address, please refer to *ITU-T Recommendation X.121* and the relevant RFC document.

Example # Configure the X.121 address of the interface Serial 2/0 as 20112451.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] x25 x121-address 20112451
```

x25 xot pvc

Syntax **x25 xot pvc** *pvc-number1 ip-address* **interface** *interface-type interface-number* **pvc** *pvc-number2* [*xot-option* | **packet-size** *input-packet output-packet* | **window-size** *input-window-size output-window-size*]*

undo x25 pvc *pvc-number1*

View Interface view

Parameter *pvc-number1*: Number of PVC on the local interface, in the range 1 to 4095.

ip-address: IP address of the peer on the XOT connection.

interface *interface-type interface-number*: Specifies an interface by its type and number.

pvc *pvc-number2*: Specifies a PVC on the peer interface. The *pvc-number2* argument is in the range 1 to 4095.

xot-option: XOT channel parameter option. For specific configuration, see Table 72.

Table 72 XOT channel parameter option

Option	Description
timer *seconds*	Keepalive timer delay of XOT connection. The timer sends the keepalive packet upon timeout to detect the connection availability. Its value ranges from 1 to 3600.
retry *times*	Number of maximum retries for sending keepalives. If the number exceeds *times*, the XOT connection will be disconnected. Its value ranges from 3 to 3600.
source *interface-type interface-number*	Type and number of the interface that initiates the XOT connection.

packet-size *input-packet output-packet*: Specifies the maximum input and output packet lengths in bytes, in the range 16 to 4,096. The sizes must be an integer power of 2.

window-size *input-window-size output-window-size*: Specifies the input and output window sizes of the VC. If the modulo of the PVC's interface is 8, the values are in the range 1 to 7; if the modulo is 128, the values are in the range 1 to 127.

Description Use the **x25 xot pvc** command to add a PVC route of XOT.

Use the **undo x25 pvc** command to delete the specified PVC route of XOT.

By default, no PVC route of XOT is configured.

XOT (X.25 Over TCP) is a protocol to load X.25 packet over TCP. Configuring the XOT switching PVC can connects the local X.25 network to the remote one over the IP network. You can also configure the keepalive attribute to support link detection.

Related command: **display x25 vc**, **x25 switching**.

Example # Configure an XOT PVC route to forward packets from PVC1 to the device at 10.1.1.2, which then forwards the packets out PVC2 on Serial 2/0.

```
<Sysname> system-view
[Sysname] x25 switching
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip address 10.1.1.1 255.255.255.0
[Sysname-Ethernet1/0] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol x25 dce ietf
[Sysname-Serial2/0] x25 xot pvc 1 10.1.1.2 interface serial 2/0 pvc 2
```

x29 timer inviteclear-time

Syntax **x29 timer inviteclear-time** *seconds*

undo x29 timer inviteclear-time

View System view

Parameter *seconds*: Delay time in seconds, in the range 5 to 2147483. The delay waiting for response after inviting PAD clear procedure.

Description Use the **x29 timer inviteclear-time** command to set the delay waiting for response after the PAD clear procedure is initiated. Upon expiration of this timer, the server aborts the connection by force and starts X.25 clear procedures.

Use the **undo x29 timer inviteclear-time** command to restore the default.

The default is 5 seconds.

The server of X.25 PAD may send an Invite Clear message to the client, for example, after receiving a quit request from client or in order to release the link. At the same time, a timer is started. If no response is received upon expiration of the timer, the server clears the link.

Example # Set the delay waiting for response after the PAD clear procedure is initiated to 1000 seconds.

```
<Sysname> system-view
[Sysname] x29 timer inviteclear-time 1000
```

27 LINK AGGREGATION CONFIGURATION COMMANDS

Link aggregation is not supported on MSR 20 series routers. It is only supported on the interfaces of 16FSW/24FSW modules of MSR 30/MSR 50 series routers.

display lacp system-id

Syntax **display lacp system-id**

View Any view

Parameter None

Description Use the **display lacp system-id** command to display the local system ID (also called the actor system ID), which comprises the system LACP priority and the system MAC address.

Example # Display the local system ID.

```
<Sysname> display lacp system-id
 Actor System ID: 0x8000, 00e0-fc00-0100
```

display link-aggregation interface

Syntax **display link-aggregation interface** *interface-type interface-number* [**to** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies a port range or a port if the **to** keyword and the second port are not specified.

Description Use the **display link-aggregation interface** command to display detailed information about link aggregation for the specified port or ports.

You may find that information about the remote system is replaced by 0 and no statistics about LACPDUs are provided for manual link aggregation groups. This is normal because this type of aggregation group has no knowledge of its partner and does not use LACP PDUs for maintaining link aggregation.

Example # Display detailed information about link aggregation for port Ethernet 1/1 in a manual aggregation group.

```
<Sysname> display link-aggregation interface ethernet 1/1
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
         D -- Synchronization, E -- Collecting, F -- Distributing,
         G -- Defaulted, H -- Expired

 Ethernet1/1:
   Selected AggID: 1
   Local:
     Port-Priority: 32768, Oper key: 1, Flag: {}
   Remote:
     System ID: 0x0, 0000-0000-0000
     Port Number: 0, Port-Priority: 0, Oper-key: 0, Flag: {}
```

Display detailed information about link aggregation for port Ethernet 1/2 in a static aggregation group.

```
<Sysname> display link-aggregation interface ethernet 1/2
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
         D -- Synchronization, E -- Collecting, F -- Distributing,
         G -- Defaulted, H -- Expired

Ethernet1/2:
   Selected AggID: 20
   Local:
     Port-Priority: 32768, Oper key: 2, Flag: {ACDEF}
   Remote:
     System ID: 0x8000, 000e-84a6-fb00
     Port Number: 2, Port-Priority: 32768 , Oper-key: 10, Flag: {ACDEF}
   Received LACP Packets: 8 packet(s), Illegal: 0 packet(s)
   Sent LACP Packets: 9 packet(s)
```

Table 73 Description on the fields of display link-aggregation interface

Field	Description
Flags	One-octet LACP state flags field. From the least to the most significant bit, they are represented by A through H as follows: ■ A indicates whether LACP is enabled, 1 for enabled and 0 for disabled. ■ B indicates the timeout control value, 1 for short timeout, and 0 for long timeout. ■ C indicates whether the sending system considers this link to be aggregatable, 1 for true, and 0 for false. ■ D indicates whether the sending system considers that this link is synchronized, 1 for true, and 0 for false. ■ E indicates whether the sending end considers that collection of incoming frames is enabled on the link, 1 for true and 0 for false. ■ F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link, 1 for true and 0 for false. ■ G indicates whether the receive state machine of the sending system is using default operational partner information, 1 for true and 0 for false. ■ H indicates whether the receive state machine of the sending system is in the expired state, 1 for true and 0 for false. If a flag bit is set to 1, the corresponding English letter that otherwise is not output displays.
Selected AggID	ID of the link aggregation group of which this port is a member
Local: Port-Priority, Oper key, Flag	Local port LACP priority, operational key, LACP state flag
Remote: System ID, Port Number, Port-Priority, Oper-key, Flag	Remote system ID, port number, port LACP priority, operational key, and LACP state flag
Received LACP Packets, Illegal, Sent LACP Packets	Statistics about received, invalid, and sent LACP packets

display link-aggregation summary

Syntax **display link-aggregation summary**

View Any view

Parameter None

Description Use the **display link-aggregation summary** command to display a summary for all link aggregation groups.

You may find that information about the remote system for a manual link aggregation group is either replaced by none or not displayed at all. This is normal because this type of aggregation group has no knowledge of its partner.

Example # Display the link aggregation group summary.

```
<Sysname> display link-aggregation summary
Aggregation Group Type: S -- Static, M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 00e0-fcff-ff04

  AL     AL  Partner ID           Select    Unselect    Share   Master
  ID     Type                     Ports Ports   Type        Port
------------------------------------------------------------------------
  10     M   none                  1        0       NonS        Ethernet1/2
  20     S   0x8000,00e0-fcff-ff01 1        0       NonS        Ethernet1/3
```

Table 74 Description on the fields of display link-aggregation summary

Field	Description
Aggregation Group Type	Aggregation group type. ■ S: static LACP aggregation ■ M: manual aggregation
Loadsharing Type	Load sharing type, which can be "Shar" (for load sharing) and "NonS" (for non-load sharing).
Actor ID	Local system ID
AL ID	Link aggregation group ID
AL Type	Link aggregation type, which can be dynamic LACP aggregation, static LACP aggregation, or manual aggregation.
Partner ID	Remote system ID
Select Ports	Number of selected ports
Unselect Ports	Number of unselected ports
Share Type	Load sharing type
Master Port	Master port

display link-aggregation verbose

Syntax **display link-aggregation verbose** [*agg-id*]

View Any view

Parameter *agg-id*: ID of an existing link aggregation group, in the range 1 to 144.

Description Use the **display link-aggregation verbose** command to display detailed information about the specified or all link aggregation groups.

You may find that information about the remote system for a manual link aggregation group is either replaced by none or not displayed at all. This is normal because this type of aggregation group has no knowledge of its partner.

Example # Display detailed information about all the link aggregation groups.

```
<Sysname> display link-aggregation verbose
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Flags:  A -- LACP_Activity, B -- LACP_timeout, C -- Aggregation,
        D -- Synchronization, E -- Collecting, F -- Distributing,
        G -- Defaulted, H -- Expired

Aggregation ID: 1,  AggregationType: Static,   Loadsharing Type: Shar
Aggregation Description:
System ID: 0x8000, 000f-e219-57c3
Port Status: S -- Selected,  U -- Unselected
Local:
  Port             Status  Priority  Oper-Key  Flag
--------------------------------------------------------------------------------
  GE1/2            S       32768     2         {ACDEF}
  GE1/3            S       32768     2         {ACDEF}

Remote:
  Actor         Partner Priority  Oper-Key  SystemID               Flag
--------------------------------------------------------------------------------
  GE1/2            161      32768      1          0x8000,00e0-fc00-12b0  {ACDEF}
  GE1/3            164      32768      1          0x8000,00e0-fc00-12b0  {ACDEF}

Aggregation ID: 2,  AggregationType: Static,   Loadsharing Type: NonS
Aggregation Description:
System ID: 0x8000, 000f-e219-57c3
Port Status: S -- Selected,  U -- Unselected
Local:
  Port             Status  Priority  Oper-Key  Flag
--------------------------------------------------------------------------------
  GE2/1            U       32768     1         {AG}

Remote:
  Actor            Partner Priority  Oper-Key  SystemID                 Flag
--------------------------------------------------------------------------------
  GE2/1            0         32768     0          0x8000,0000-0000-0000  {EF}
```

Table 75 Description on the fields of display link-aggregation verbose

Field	Description
Loadsharing Type	Load sharing type, either shar for loadsharing or NonS for non-load sharing

Table 75 Description on the fields of display link-aggregation verbose

Field	Description
Flags	One-octet LACP flags field indicates the actor state variables for the port. From the least to the most significant bit, they are represented by A through H as follows: ■ A indicates the enabling/disabling state of LACP, 1 for enabled and 0 for disabled ■ B indicates the timeout control value, 1 for short timeout, and 0 for long timeout ■ C indicates whether the sending system considers this link to be aggregatable, 1 for true, and 0 for false ■ D indicates whether the sending system considers that this link is synchronized, 1 for true, and 0 for false ■ E indicates whether the sending system considers that collection of incoming frames is enabled on the link, 1 for true and 0 for false ■ F indicates whether the sending system considers that distribution of outgoing frames is enabled on the link, 1 for true and 0 for false ■ G indicates whether the receive state machine of the sending system is using default operational partner information, 1 for true and 0 for false ■ H indicates whether the receive state machine of the sending system is in the expired state, 1 for true and 0 for false If a flag bit is set to 1, the corresponding English letter that otherwise is not output displays.
Aggregation ID	Link aggregation group ID
AggregationType	Link aggregation type: manual LACP or static LACP
Aggregation Description	Link aggregation group name
System ID	Local system ID
Port State	Port state in a link aggregation group: selected or unselected
Local: Port, Status, Priority, Oper-key, Flag	Other information about the local end, including member ports, port state, port LACP priority, operational key, and flags
Remote: Actor, Partner, Priority, Oper-key, SystemID, Flag	Detailed information about the remote end, including corresponding local port, port ID, port LACP priority, operational key, system ID, and flags

lacp port-priority

Syntax **lacp port-priority** *port-priority*

undo lacp port-priority

View Ethernet interface view

Parameter *port-priority*: Port LACP priority, in the range 0 to 65535.

Description Use the **lacp port-priority** command to assign an LACP priority to the port.

Use the **undo lacp port-priority** command to restore the default.

By default, port LACP priority is 32768.

Related command: **display link-aggregation interface**, **display link-aggregation verbose**.

Example # Assign LACP priority 64 to a port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] lacp port-priority 64
```

lacp system-priority

Syntax **lacp system-priority** *system-priority*

undo lacp system-priority

View System view

Parameter *system-priority*: System LACP priority, in the range 0 to 65535.

Description Use the **lacp system-priority** command to assign an LACP priority to the local system.

Use the **undo lacp system-priority** command to restore the default.

By default, system LACP priority is 32768.

Example # Assign LACP priority 64 to the local system.

```
<Sysname> system-view
[Sysname] lacp system-priority 64
```

link-aggregation group description

Syntax **link-aggregation group** *agg-id* **description** *agg-name*

undo link-aggregation group *agg-id* **description**

View System view

Parameter *agg-id*: Link aggregation group ID, in the range 1 to 144.

agg-name: Link aggregation group name, a string of 1 to 32 characters.

Description Use the **link-aggregation group description** command to configure a name for the specified link aggregation group.

Use the **undo link-aggregation group description** command to remove the name of the specified link aggregation group.

Related command: **display link-aggregation verbose**.

Example # Name link aggregation group 22 as abc.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 description abc
```

link-aggregation group mode

Syntax **link-aggregation group** *agg-id* **mode** { **manual** | **static** }

undo link-aggregation group *agg-id*

View System view

Parameter *agg-id*: Link aggregation group ID, in the range 1 to 144.

manual: Creates a manual link aggregation group.

static: Creates a static LACP link aggregation group.

Description Use the **link-aggregation group mode** command to create a link aggregation group.

Use the **undo link-aggregation group** command to remove a link aggregation group.

Note that aggregation groups currently referenced by modules cannot be removed.

Related command: **display link-aggregation summary**.

Example # Create manual link aggregation group 22.

```
<Sysname> system-view
[Sysname] link-aggregation group 22 mode manual
```

port link-aggregation group

Syntax **port link-aggregation group** *agg-id*

undo port link-aggregation group

View Ethernet interface view

Parameter *agg-id*: Link aggregation group ID, in the range 1 to 144.

Description Use the **port link-aggregation group** command to add the Ethernet port to a link aggregation group (manual or static LACP).

Use the **undo port link-aggregation group** command to remove the Ethernet port from a link aggregation group.

Related command: **display link-aggregation verbose**.

Example # Assign port Ethernet 1/0 to link aggregation group 22.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-aggregation group 22
```

port-group aggregation

Syntax **port-group aggregation** *agg-id*

View System view

Parameter *agg-id*: Aggregation port group ID, in the range 1 to 144.

Description Use the **port-group aggregation** command to enter aggregation port group view.

Instead of being created administratively, an aggregation port group is created automatically upon creation of a link aggregation group and assigned the ID of the link aggregation group. In aggregation port group view, you can configure aggregation related settings such as STP, VLAN, QoS, GVRP, and MAC address learning, but cannot add or remove member ports.

Example # Enter aggregation port group view.

```
<Sysname> system-view
[Sysname] port-group aggregation 10
[Sysname-port-group-aggregation-10]
```

reset lacp statistics

Syntax **reset lacp statistics** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Parameter **interface** *interface-type interface-number* [**to** *interface-type interface-number*]: Specifies an interface range or an interface if the **to** keyword and the second interface are not specified.

Description Use the **reset lacp statistics** command to clear statistics about LACP on a specified port or ports.

Related command: **display link-aggregation interface**.

Example # Clear statistics about LACP on all ports.

```
<Sysname> reset lacp statistics
```

28 LINK AGGREGATION DEBUGGING COMMANDS

debugging lacp packet

Syntax **debugging lacp packet** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

undo debugging lacp packet [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]]

View User view

Default Level 1: Monitor level

Parameters *interface-type interface-number*: Port type and port number.

to: Specifies the ports with their port type and port number within the port range enclosed by the two *interface-type-interface-number* argument pairs around this keyword.

Description Use the **debugging lacp packet** command to enable debugging for LACP protocol packets on the specified port(s).

Use the **undo debugging lacp packet** command to disable debugging for LACP protocol packets on the specified port(s).

By default, debugging for LACP protocol packets is disabled on a port.

If no port is specified, the command applies to all the ports running LACP.

Table 76 Description on the fields of the debugging lacp packet command

Field	Description
size	Size of a protocol packet, which is 128 bytes.
subtype	Sub type of a protocol packet, which is 1 for LACP protocol packets.
version	Protocol version, which is 1 for LACP.

Table 76 Description on the fields of the debugging lacp packet command

Field	Description
Actor	Local port information carried in the protocol packet, which contains the following fields. ■ **tlv**: A value of 1 indicates that the information is about the local port. ■ **len**: The length of the Actor information. ■ **sys-pri**: The LACP priority of the system where the local port resides. ■ **sys-mac**: The system MAC address of the system where the local port resides. ■ **key**: The value of the operation key of the local port. ■ **pri**: The LACP priority of the local port. ■ **p**: The local port number. ■ **state**: The current LACP state of the local port.
Partner	Peer port information carried in the protocol packet, which contains the following fields. ■ **tlv**: A value of 2 indicates that the information is about the peer port. ■ **len**: The length of the Partner information. ■ **sys-pri**: The LACP priority of the system where the peer port resides. ■ **sys-mac**: The system MAC address of the system where the peer port resides. ■ **key**: The value of the operation key of the peer port. ■ **pri**: The LACP priority of the peer port. ■ **p**: The peer port number. ■ **state**: The current LACP state of the peer port.
Collector	The content of the Collector field carried in the protocol packet, which contains the following fields. ■ **tlv**: A value of 3 indicates the Collector field. ■ **len**: The length of the Collector field. ■ **col-max-delay**: The maximum delay.
Terminator	The content of the Terminator field carried in the protocol packet, which contains the following fields. ■ **tlv**: A value of 0 indicates the Terminator field, which marks the end of the protocol packet. ■ **len**: The length of the Terminator field.

Examples # Enable debugging for LACP protocol packets on Ethernet 1/1 to view the information about LACP protocol packet sending/receiving of the port.

```
<Sysname> debugging lacp packet interface ethernet 1/1
*0.60323 Sysname LAGG/8/Pkt:
 Send LACP Packet via port Ethernet1/1
```

// The device sent an LACP protocol packet through Ethernet 1/1.

```
*0.60323 Sysname LAGG/8/Pkt:
 size=128, subtype =1, version=1
```

// The length of the LACP packet was 128 bytes, the protocol sub type was 1, and the version number was 1.

```
Actor: tlv=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=0x
1, pri=0x8000, p=0x2, state=0x45
```

// The local port information carried in the packet was as follows:

- *length: 20*
- *system LACP priority: 0x8000*
- *system MAC address: 00e0-fc02-0300*
- *port operation key: 0x1*
- *port LACP priority: 0x8000*
- *port number: 0x2*
- *current LACP state flag of the port: 0x45*

```
Partner: tlv=2, len=20, sys-pri=0x0, sys-mac=0000-0000-0000, key=0x0
, pri=0x0, p=0x0, state=0x0
```

// The peer port information carried in the packet was as follows:

- *length: 20*
- *system LACP priority: 0x0*
- *system MAC address: 0000-0000-0000*
- *port operation key: 0x0*
- *port LACP priority: 0x0*
- *port number: 0x0*
- *current LACP state flag of the port: 0x0*

```
Collector: tlv=3, len=16, col-max-delay=0
```

// The content of the Collector field in the protocol packet was as follows:

- *length: 16*
- *maximum delay: 0*

```
Terminator: tlv=0, len=0
```

// The length of the Terminator field in the protocol packet is 0.

```
*0.1221133 Sysname LAGG/8/Pkt:
 Receive LACP Packet via port Ethernet1/1
```

// The device received an LACP protocol packet through Ethernet 1/1.

```
*0.1221133 Sysname LAGG/8/Pkt:
 size=128, subtype =1, version=1
```

// The length of the LACP packet was 128 bytes, the protocol sub type was 1, and the version number was 1.

```
Actor: tlv=1, len=20, sys-pri=0x8000, sys-mac=00e0-fc00-0000, key=0x
1, pri=0x8000, p=0x6, state=0x3d
```

// The local port information carried in the packet was as follows:

- *length: 20*
- *system LACP priority: 0x8000*
- *system MAC address: 00e0-fc00-0000*
- *port operation key: 0x1*
- *port LACP priority: 0x8000*
- *port number: 0x6*
- *current LACP state flag of the port: 0x3d*

```
Partner: tlv=2, len=20, sys-pri=0x8000, sys-mac=00e0-fc02-0300, key=
0x1, pri=0x8000, p=0x1, state=0xd
```

// The peer port information carried in the packet was as follows:

- *length: 20*
- *system LACP priority: 0x0*
- *system MAC address: 00e0-fc02-0300*
- *port operation key: 0x1*
- *port LACP priority: 0x8000*
- *port number: 0x1*
- *current LACP state flag of the port: 0xd*

```
Collector: tlv=3, len=16, col-max-delay=0
```

// The content of the Collector field in the protocol packet was as follows:

- *length: 16*
- *maximum delay: 0*

```
Terminator: tlv=0, len=0
```

// The length of the Terminator field in the protocol packet is 0.

Other similar LACP protocol packet information is omitted here.

debugging lacp state

Syntax **debugging lacp state** [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** } * | **all** }

undo debugging lacp state [**interface** *interface-type interface-number* [**to** *interface-type interface-number*]] { { **actor-churn** | **mux** | **partner-churn** | **ptx** | **rx** } * | **all** }

View User view

Default Level 1: Monitor level

Parameters *interface-type interface-number*: Port type and port number.

to: Specifies the ports with their port type and port number within the port range enclosed by the two *interface-type-interface-number* argument pairs around this keyword.

actor-churn: Debugging for Actor-churn state machine.

mux: Debugging for MUX state machine.

partner-churn: Debugging for Partner-churn state machine.

ptx: Debugging for PTX state machine.

rx: Debugging for RX state machine.

all: Debugging for all the state machines.

Description Use the **debugging lacp state** command to enable debugging for LACP protocol state machines on the specified port(s).

Use the **undo debugging lacp state** command to disable debugging for LACP protocol state machines on the specified port(s).

By default, debugging for LACP protocol state machines is disabled on a port.

If no port is specified, the command applies to all the ports running LACP.

Table 77 Description on the fields of the debugging lacp state command

Field	Description
from state XXX	The original state of a state transition
to state XXX	The final state of the state transition
stimulation	The event that triggers the state transition

Examples # Enable debugging for Rx state machine on Ethernet 2/1 to view the information about LACP Rx state transition.

```
<Sysname> debugging lacp state interface ethernet 1/2 rx
*0.1360830 Sysname LAGG/8/FSM:
 Port Ethernet1/2: FSM Rx  transfers from state RESERVE to state INITIALIZE
 by the stimulation Begin_True
```

// RX state machine was initiated and then transited to the INITIALIZE state. The event that triggered the transition was the startup of the state machine (Begin_True).

```
*0.1360830 Sysname LAGG/8/FSM:
Port Ethernet1/2: FSM Rx  transfers from state INITIALIZE to state PORT_DISABLED
 by the stimulation UCT
```

// RX state machine transited from the INITIALIZE state to the PORT_DISABLED state unconditionally (identified by UCT).

```
*0.1360830 Sysname LAGG/8/FSM:
Port Ethernet1/2: FSM Rx  transfers from state PORT_DISABLED to stat
e EXPIRED by the stimulation Lacp_Enabled
```

// RX state machine transited from the PORT_DISABLED state to the EXPIRED state. The event that triggered the transition was the enabling of LACP (Lacp_Enabled).

```
*0.1360862 Sysname LAGG/8/FSM:
 Port Ethernet1/2: FSM Rx  transfers from state EXPIRED to state CURRENT
 by the stimulation Pdu_Indicate
```

// RX state machine transited from the EXPIRED state to the CURRENT state (normal running state). The event that triggered the transition was the reception of the protocol packets from the peer (Pdu_Indicate).

debugging link-aggregation error

Syntax **debugging link-aggregation error**

undo debugging link-aggregation error

View User view

Default Level 1: Monitor level

Parameters None

Description Use the **debugging link-aggregation error** command to enable debugging for link aggregation errors.

Use the **undo debugging link-aggregation error** command to disable debugging for link aggregation errors.

By default, debugging for link aggregation errors is disabled.

Table 78 Description on the fields of debugging link-aggregation error command

Field	Description
File	The program file that incurs a running error
Line	The number of the line where the error occurs
ERROR	Error description

Examples # Enable debugging for link aggregation errors to view the error information prompted during the system running.

```
<Sysname> debugging link-aggregation error
*0.21953 Sysname LAGG/8/lacpErrorEvent:
 File e:v500d05sp1softwarelacplacp_agm.c, Line: 1200
 ERROR------  Portindex: 1   LACP_SendLACPPacket ,g_ucLacpSysMAC NULL !
```

// File e:v500d05sp1softwarelacplacp_agm.c has a running error, which occurs at line 1200. The ERROR field indicated that the system MAC address obtained is null.

debugging link-aggregation event

Syntax **debugging link-aggregation event**

undo debugging link-aggregation event

View User view

Default Level 1: Monitor level

Parameters None

Description Use the **debugging link-aggregation event** command to enable debugging for link aggregation events.

Use the **undo debugging link-aggregation event** command to disable debugging for link aggregation events.

By default, debugging for link aggregation events is disabled.

Table 79 Description on the fields of debugging link-aggregation event command

Field	Description
Agg Index	Aggregation group ID
Cfg MD5	MD5 digest
Restriction Value	Hardware restriction parameter
Admin Key	Administration key
Port Pri	Port LACP priority
Sys Mac	System MAC address
Sys Pri	System LACP priority
Oper Key	Port operation key

Examples # Enable debugging for link aggregation events to view the information about the events concerning link aggregation groups.

```
<Sysname> debugging link-aggregation event
<Sysname> display  link-aggregation summary

Aggregation Group Type: S -- Static , M -- Manual
Loadsharing Type: Shar -- Loadsharing, NonS -- Non-Loadsharing
Actor ID: 0x8000, 00e0-fc57-367f

  AL  AL   Partner ID          Select Unselect Share Master
  ID  Type                       Ports  Ports    Type  Port
--------------------------------------------------------------------------------
  10  M    none                  1      0        NonS  Ethernet1/1
```

// Aggregation group 10 existed. It contained Ethernet 1/1.

Remove aggregation group 10.

```
<Sysname> system-view
[Sysname] undo link-aggregation group 10
*0.91991886 Sysname LAGG/8/AggDel:Link Aggregation 10 is deleted.
```

// Aggregation group 10 was removed.

```
*0.91991961 Sysname LAGG/8/OperKeyDel:Oper key 1 is deleted.
```

// The operation key of port Ethernet 1/1 (Key 1) was removed.

```
*0.91992115 Sysname LAGG/8/AggDel:Slot=2;Link Aggregation 10 is dele
ted.
```

// Aggregation group 10 was removed on interface card 2.

29 MODEM CONFIGURATION COMMANDS

modem

Syntax **modem** [**both** | **call-in** | **call-out**]

undo modem [**both** | **call-in** | **call-out**]

View User interface view

Parameter **both**: Permits both modem call-in and modem call-out.

call-in: Permits only modem call-in.

call-out: Permits only modem call-out.

Description Use the **modem** command to enable modem call-in and call-out on the interface.

Use the **undo modem** command to disable modem call-in or call-out.

By default, both modem call-in and call-out are disabled on the interface.

Example # Enable receiving incoming Modem calls on User-interface 1.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] modem call-in
```

modem auto-answer

Syntax **modem auto-answer**

undo modem auto-answer

View User interface view

Parameter None

Description Use the **modem auto-answer** command to have the external modem connected to the asynchronous interface automatically answer or hook off.

Use the **undo modem auto-answer** command to disable the connected external modem to answer automatically. In this case, the modem answers only when receiving an AT command sent by software.

By default, the connected external modem is set to non-auto answer mode.

Use this command depending on the answer state of the connected external modem. When the modem is in auto-answer mode (AA LED of the modem lights), configure the **modem auto-answer** command to prevent the router from sending an answer command after the modem answers automatically. If the modem is in non-auto answer mode, configure the **undo modem auto-answer** command.

If the configuration of this command is not consistent with the current answer state of the connected modem, anomalies may occur. You are not encouraged to configure this command.

Example # Set the answer mode of the modem connected to the asynchronous serial interface User-interface1 to auto.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] modem auto-answer
```

modem timer answer

Syntax **modem timer answer** *time*

undo modem timer answer

View User interface view

Parameter *time:* Timeout time, in the range 1 to 60 seconds.

Description Use the **modem timer answer** command to set the interval from user hookoff to dial.

Use the **undo modem timer answer** command to restore the default.

By default, the valid interval is 30 seconds.

This command is only valid for AUX interface and other asynchronous interfaces.

Example # Set the valid interval from user hookoff to dial to 50 seconds.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem timer answer 50
```

sendat

Syntax **sendat** *at-string*

View Interface view (The interface can be an asynchronous serial interface, a asynchronous/synchronous serial interface operating in the asynchronous mode, an AUX interface, or an AM interface.)

Parameter *at-string*: AT command string. This argument can contain "+++", "A/" or any string beginning with AT.

For detailed description of AT commands, see Table 80

Description Use the **sendat** command to send AT command to modem manually.

The **sendat** command sends strings to modem as AT commands without checking whether or not the strings are valid commands. The characters that are in lowercase in the string are converted to the corresponding uppercase characters automatically.

If debugging for modem is enabled on the interface, the result code returned by modem is displayed. If you specify to display the executed commands, The AT commands executed are displayed as well.

- *To accept AT commands from the modem, you must first put the modem in AT command mode. So sending commands in transmitting mode is invalid.*
- *The **sendat** command can issue only one AT command at a time.*
- *After Modem is configured with the AT command, its operating state might be changed, thus affecting the functions such as dialup. Please use this function with caution under the guidance of technicians.*

Table 80 Description on common AT commands

Command	Description
AT	Commands used to configure a modem, except A/ (Repeat Last Command) and +++ (Escape Code), begin with **AT**. **AT** informs the modem that commands are being sent to it. If you execute the AT command only, the modem returns OK or 0, which indicates that it is ready to accept commands.
A	Use **A** command to enable a modem to answer an incoming call without waiting for the ringing. You can use this command when you configure to answer an incoming call manually or the modem is configured to connect to another modem in actively. All the commands following the **A** command in the same command line are ignored.

Table 80 Description on common AT commands

Command	Description
Bn	Specifies the communication standard to be adopted and the transmission speed. The communication standard can be ITU or Bell. The n argument can be 0, 1, 2/3, 15, or 16.
	B0 specifies ITU V.22 and sets the transmission speed to 1,200 bps.
	B1 specifies Bell 212 and sets the transmission speed to 1,200 bps, which is a default setting.
	B2/B3 disables ITU V23 return path.
	B15 specifies ITU V21 and sets the transmission speed to 3,000 bps.
	B16 specifies 103J and sets the transmission speed to 300 bps, which is a default setting.
En	Sets the modem to echo commands to the workstation. The n argument can be o or 1.
	E0 disables echo of commands to the workstation.
	E1 enables echo of commands to the workstation, which is a default setting.
Dn	Dial Command enables the modem to dial the number following D in the command line. In the mode of pulse dialing, the modem ignores nonnumeric characters.
Hn	Hang up Control specifies the way to hang up a modem,
	H0 hangs up a modem, which is a default setting.
	H1 disconnects a modem through off hook.
In	Inquiries to display the modem product ID, ROM checksum or ROM checksum status. The n argument can be 0/3, 1, 2, 4, 5 or 9.
	I0/I3 displays the default speed and hardware version of controller in the modem.
	I1 calculates and displays ROM checksum.
	I2 checks ROM, calculates and checks checksum, and displays the information of OK or ERROR.
	I4 displays hardware version of data pump.
	I5 displays the ID, software version, hardware version and the country code of modem board.
	I9 displays the country code.
Ln	Specifies the speaker volume to low, medium and high. The n argument ranges from 0 to 3.
	L0/L1 sets the volume to be low.
	L2 sets the volume to be medium.
	L3 sets the volume to be high.
Mn	Monitors a speaker to be on or off when faxing and communicating. The n argument ranges from 0 to 3.
	M0 sets a speaker to be off.
	M1 sets a speaker to be on before carrier signal is detected, M1 is a default setting.
	M2 sets a speaker to be on when modem is disconnected.
	M3 sets a speaker to be on before carrier signal is detected except the span of dialing.

Table 80 Description on common AT commands

Command	Description
Nn	Specifies the local modem to perform negotiation connected with remote modem of different speed. The n argument is 0 or 1. **N0** adopts the communication standard specified by S37 register and ATB commands to perform digital switch during sending or receiving calling. **N1** adopts the transmission speed specified by S37 register and ATB commands to negotiate.
On	Forces a modem to be in the online mode. The n argument can be 0, 1 or 3. **O0** sets a modem to be in online mode. **O1** Initiates the balance and reorganizes the sequences before returns to the online mode. **O3** Negotiates the transmission speed before returns to the online mode. Note that this command causes a modem to operate in the online mode again after you switch to the command mode by executing the +++ (Escape Code) command,
Qn	Enables modem to send result codes. The n argument can be 0 or 1. **Q0** enables output result codes, which is a default setting. **Q1** disables output result codes.
Sr=n	Sets the value of a specified register to be n. You can use this command to modify the value of a specified register. You can specify the register to be set by specifying the r argument. The r argument is a number that can be one among 0 through 27, 29, 31 through 33, 35, 37, and 89. The n argument is the value assigned to the register, which ranges from 0 to 255.
T	Specifies to perform tone dialing (the default). This command can also be used as the dialing corrector.
P	Specifies to perform pulse dialing. After you execute this command, a modem performs pulse dialing until you execute the **T** command. This command can also be used as the dialing corrector.
Vn	Specifies format of result codes returned by modem. The n argument can be 0 or 1. **V0** sends result codes (numeric). **V1** sends result codes (text), which is a default setting.

Example # Send dialing command to call number 169.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] physical-mode async
[Sysname-Serial2/0] sendat ATD169
```

service modem-callback

Syntax **service modem-callback**

undo service modem-callback

View System view

Parameter None

Description Use the **service modem-callback** command to enable the callback function of modems.

Use the **undo service modem-callback** command to disable the callback function of modems.

By default, the callback function of modems is disabled.

When a modem line is active, that is, when the modem detects the carrier or data is being received, you may enable callback. As the **service modem-callback** command uses modem scripts to implement callback before entering PPP, it enables callback before accounting is started. This can thus help you save cost.

Example # Enable the callback function.

```
<Sysname> system-view
[Sysname] service modem-callback
```

30 PORT MIRRORING CONFIGURATION COMMANDS

display mirroring-group

Syntax **display mirroring-group** { *groupid* | **local** }

View Any view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

local: Specifies local port mirroring groups.

Description Use the **display mirroring-group** command to display the information about a port mirroring group.

The output information varies with port mirroring group type and is organized by mirroring group numbers.

Example # Display the information about all the port mirroring groups.

```
<Sysname> display mirroring-group local
mirroring-group 3:
type: local
status: active
mirroring port:
Ethernet1/1 inbound
    Ethernet1/2 both
monitor port : Ethernet1/3
```

Table 81 Description on the fields of the display mirroring-group command

Field	Description
mirroring-group	Port mirroring group number
type	Port mirroring group type
status	Status of a port mirroring group. "Active" for already effective, and "inactive" for not effective yet.
mirroring port	Source mirroring port
monitor port	Destination mirroring port

mirroring-group

Syntax **mirroring-group** *groupid* **local**

undo mirroring-group { *groupid* | **local** }

View System view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

local: Creates a local port mirroring group/removes all local port mirroring groups.

Description Use the **mirroring-group** command to create a port mirroring group.

Use the **undo mirroring-group** command to remove the specified port mirroring group or all local port mirroring groups.

Example # Create a local port mirroring group numbered 1.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
```

mirroring-group mirroring-port

Syntax **mirroring-group** *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

undo mirroring-group *groupid* **mirroring-port** *mirroring-port-list* { **both** | **inbound** | **outbound** }

View System view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

mirroring-port-list: List of ports to be added to the port mirroring group. You can specify multiple ports by providing this argument in the form of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-8>, where the *interface-type* argument is port type, the *interface-number* argument is the port number, and &<1-8> means that you can provide up to eight port indexes/port index lists for this argument.

both: Specifies to mirror both inbound and outbound packets.

inbound: Specifies to mirror inbound packets only.

outbound: Specifies to mirror outbound packets only.

Description Use the **mirroring-group mirroring-port** command to add ports to a port mirroring group as source ports.

Use the **undo mirroring-group mirroring-port** command to remove source ports from a port mirroring group.

Note that:

- Layer 2 Ethernet ports, Layer 3 Ethernet interfaces, POS interfaces, and CPOS interfaces can all be source mirroring ports of local port mirroring groups.
- When you use the **undo mirroring-group mirroring-port** command to remove source ports from a port mirroring group, make sure the **both/inbound/outbound** keyword specified matches the actual packet direction of the ports.

Example # Add port Ethernet1/1 through Ethernet1/23 to port mirroring group 1 as source ports (assuming that port mirroring group 1 already exists).

```
<Sysname> system-view
[Sysname] mirroring-group 1 mirroring-port ethernet 1/1 to ethernet 1/23 both
```

[Sysname] mirroring-group 1 mirroring-port pos 5/1 to pos 5/4 both

[Sysname] mirroring-group 1 mirroring-port cpos 6/1 to cpos 6/4 both

Remove port Ethernet1/1 through Ethernet1/10 from port mirroring group 1.

```
[Sysname] undo mirroring-group 1 mirroring-port ethernet 1/1 to ethe
rnet 1/10 both
```

[Sysname] undo mirroring-group 1 mirroring-port pos 5/1 to pos 5/2 both

```
[Sysname] undo mirroring-group 1 mirroring-port cpos 6/1 to cpos 6/2 both
```

mirroring-group monitor-port

Syntax **mirroring-group** *groupid* **monitor-port** *monitor-port-id*

undo mirroring-group *groupid* **monitor-port** *monitor-port-id*

View System view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

monitor-port-id: Port index, in the form of *interface-type interface-number*.

Description Use the **mirroring-group monitor-port** command to add a port to a port mirroring group as the destination port.

Use the **undo mirroring-group monitor-port** command to remove the destination port from a port mirroring group.

Note that:

- A port mirroring group can contain only one destination port.
- Before add the destination port for a port mirroring group, make sure the port mirroring group exists.

- Layer 2 Ethernet ports, Layer 3 Ethernet interfaces, and tunnel interfaces can all be destination mirroring ports of local port mirroring groups.
- Member ports of an existing port mirroring group cannot be destination ports.

Example # Add port Ethernet1/1 to port mirroring group 1 (a remote destination port mirroring group) as the destination port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 monitor-port ethernet 1/1
```

mirroring-port

Syntax **[mirroring-group** *groupid* **] mirroring-port { both | inbound | outbound }**

undo [mirroring-group *groupid* **] mirroring-port { both | inbound | outbound }**

View Interface view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

both: Mirrors both inbound and outbound packets.

inbound: Mirrors the inbound packets only.

outbound: Mirrors the outbound packets only.

Description Use the **mirroring-port** command to add the current port to a port mirroring group as a source mirroring port.

Use the **undo mirroring-port** command to remove the configuration.

Note that:

- If you do not specify the **mirroring-group** *groupid* keyword-argument combination, these two commands apply to port mirroring group 1.
- Depending on device models, you can add ports/interfaces to local port mirroring groups as source mirroring ports in Layer 2 Ethernet port view, Layer 3 Ethernet interface view, POS interface view, and CPOS interface view.
- When you use the **undo mirroring-port** command to remove the current port from a port mirroring group, make sure the **both/inbound/outbound** keyword specified matches the actual packet direction of the port.

Example # Add port Ethernet1/1 to port mirroring group 2, which already exists.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] mirroring-group 2 mirroring-port both
```

Add POS 5/1 to local port mirroring group 3.

```
<Sysname> system-view
[Sysname] mirroring-group 3 local
[Sysname] interface pos 5/1
[Sysname-Pos5/1] mirroring-group 3 mirroring-port both
```

Add CPOS 6/1 to local port mirroring group 4.

```
<Sysname> system-view
[Sysname] mirroring-group 4 local
[Sysname] controller cpos 6/1
[Sysname-Cpos6/1] mirroring-group 4 mirroring-port both
```

monitor-port

Syntax [**mirroring-group** *groupid*] **monitor-port**

undo [**mirroring-group** *groupid*] **monitor-port**

View Interface view

Parameter *groupid*: Port mirroring group number. The value range is 1 to 5 for MSR 20 and BSR 30 series routers and 1 to 10 for MSR 50 series routers.

Description Use the **monitor-port** command to add the current port to a port mirroring group as the destination mirroring port.

Use the **undo monitor-port** command to remove the configuration.

If you do not specify the **mirroring-group** *groupid* keyword-argument combination, the **monitor-port** command adds the current port to port mirroring group 1.

Note that:

- Depending on device models, you can add ports/interfaces to local port mirroring groups as destination mirroring ports in Layer 2 Ethernet port view, Layer 3 Ethernet interface view, and tunnel interface view.
- Member ports of an existing port mirroring group cannot be destination ports.

Example # Add port Ethernet 1/1 to port mirroring group 1 (a local port mirroring group) as the destination port.

```
<Sysname> system-view
[Sysname] mirroring-group 1 local
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] monitor-port
```

31 PPP AND MP CONFIGURATION COMMANDS

display interface mp-group

Syntax **display interface mp-group** [*mp-number*]

View Any view

Parameter *mp-number*: Multilink point to point protocol group (MP-group) interface number, which can be the number of any existing MP-group interface.

Description Use the **display interface mp-group** command to view the information about an existing MP-group interface. If the *mp-number* argument is not specified, the information about all existing MP-group interfaces is displayed.

Example # View the information about the interface MP-group 12.

```
<Sysname> display interface mp-group 12
Mp-group12 current state: DOWN
Line protocol current state: DOWN
Description: Mp-group12 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is MP
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Table 82 Description on the fields of the display interface mp-group command

Field	Description
current state	Physical state of the interface (up or down)
Line protocol current state	State of the data link layer protocol (up or down)
Description	Description string of the interface
The Maximum Transmit Unit	Maximum transmit unit (MTU) of the interface
Hold timer	Hold time of the link state (up/down) of the current interface
Internet protocol processing	State of the network layer protocol (enabled or disabled)

Table 82 Description on the fields of the display interface mp-group command

Field	Description
LCP initial	Link control protocol (LCP) negotiation is complete
Physical	Physical type of the interface
Last 300 seconds input: 0 bytes/sec 0 packets/sec	Average rate of input packets and output packets in the last 300 seconds (in bps)
Last 300 seconds output: 0 bytes/sec 0 packets/sec	
0 packets input, 0 bytes, 0 drops	Total amount of input packets of the interface (in the number of packets and in bytes respectively), and the number of dropped packets within the input packets
0 packets output, 0 bytes, 0 drops	Total amount of output packets of the interface (in the number of packets and in bytes respectively), and the number of dropped packets within these output packets

display interface virtual-template

Syntax **display interface virtual-template** [*number*]

View Any view

Parameter *number*: Virtual template (VT) number, which can be the number of any existing VT.

Description Use the **display interface virtual-template** command to view the information about a VT. If you do not provide the *number* argument, this command will display the information about all the existing VTs.

Related command: **interface virtual-template**.

Example # View the information about VT 1.

```
<Sysname> display interface virtual-template 1
Virtual-Template1 current state: UP
Line protocol current state: UP (spoofing)
Description: Virtual-Template1 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is None
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Refer to Table 82 for the description on the other fields.

display ppp mp

Syntax **display ppp mp** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ppp mp** command to display information and statistics of MP interfaces.

Related command: **link-protocol ppp**, **ppp mp**.

Example # Display the information about MP interfaces configured through the MP-group.

```
<Sysname> display ppp mp
Mp-group is Mp-group0
max-bind: 20, min-fragment: 128 ,LFI max-delay: 100

 Bundle Multilink, 6 members, slot 0, Master link is Mp-group0
 Peer's endPoint descriptor: 1e9935f57c85
 Bundle Up Time: 2005/03/13  19:54:23:60
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 The member channels bundled are:
      Serial1/1:15     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:16     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:17     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:18     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:19     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:20     Up-Time:2005/03/13  19:54:23:60
 Inactive member channels: 4 members
      Serial1/1:21     (inactive)
      Serial1/1:22     (inactive)
      Serial1/1:23     (inactive)
      Serial1/1:24     (inactive)
```

Table 83 Description on the fields of the display ppp mp command

Field	Description
Mp-group is Mp-group0	The MP-group interface is MP-group0.
max-bind	Maximum number of links in a MP bundle
min-fragment	Minimum size of an MP fragment
LFI max-delay	Maximum delay to transmit an LFI fragment
Bundle Multilink	Endpoint MP username is Multilink
6 member	Six channels are bound.
slot 0	The channels are bound on slot 0.
Master link is MP-group0	The master channel is MP-group0.
Peer's endPoint descriptor: 1e9935f57c85	The endpoint descriptor of the peer is 1e9935f57c85.
Bundle Up Time: 2005/03/13 19:54:23:60	The MP channel went up at 19:54:23:60 on March 13, 2005.
0 lost fragments	Number of the lost fragments

Table 83 Description on the fields of the display ppp mp command

Field	Description
0 reordered	Number of the packets reassembled
0 unassigned	Number of the packets waiting for being reassembled
0 interleaved	Number of the interleaved packets
sequence 0/0 rcvd/sent	Received sequence number/sent sequence number
The member channels bundled are	The following displays all the member channels bundled on this logical channel
Serial1/1:15 Up-Time:2005/03/13 19:54:23:60	Subchannel Serial1/1:15 is up at 19:54:23:60 on March 13, 2005
Inactive member channels	List of inactive subchannels

Display information about MP interfaces, which are configured via MP-groups.

```
<Sysname> display ppp mp
Mp-group is Mp-group0
max-bind: 20, min-fragment: 128 ,LFI max-delay: 100

 Bundle Multilink, slot 0, Master link is Mp-group0
 Peer's endPoint descriptor: 1e9935f57c85
 Bundle Up Time: 2005/03/13  19:54:23:60
  0 lost fragments, 0 reordered, 0 unassigned, 0 interleaved,
 sequence 0/0 rcvd/sent
 Member channels: 6 active, 4 inactive
      Serial1/1:15     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:16     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:17     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:18     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:19     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:20     Up-Time:2005/03/13  19:54:23:60
      Serial1/1:21     (inactive)
      Serial1/1:22     (inactive)
      Serial1/1:23     (inactive)
      Serial1/1:24     (inactive)
```

For description on the output fields, refer to Table 83.

display virtual-access

Syntax **display virtual-access** [*va-number* | **dialer** *dialer-number* | **peer** *peer-address* | **user** *user-name* | **vt** *vt-number*] *

View Any view

Parameter *va-number*: VA interface number, in the range 0 to 128.

dial *dialer-number*: Specifies a dialer interface number, which is in the range of 0 to 1023.

peer *peer-address*: Specifies the IP address of the peer of the VA interface, expressed in dotted decimal notation.

user *user-name*: Specifies a user name used for logging in through the VA interface. The *user-name* argument is a string of 1 to 80 characters.

vt *vt-number*: Specifies the number of the VT associated to the virtual access (VA) interface. The *user-name* argument ranges from 0 to 1023.

Description Use the **display virtual-access** command to view the information about specific VA interfaces.

VA interfaces are created automatically by the system, and they adopt the settings of specific VTs. A VA interface can be removed due to failures of lower layer connections or user intervention.

Example # Display the information about all the VA interfaces adopting the settings of VT 1.

```
<Sysname> display virtual-access vt 1
Virtual-Template1:0 current state :UP
Line protocol current state :UP
Description : Virtual-Template1:0 Interface
The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened, OSICP opened
Physical is MP, baudrate: 64000
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Refer to Table 82 for the description on the fields of the **display interface virtual-access** command.

interface mp-group

Syntax **interface mp-group** *mp-number*

undo interface mp-group *mp-number*

View System view

Parameter *mp-number*: MP group interface number, ranging from 0 to 1023.

Description Use the **interface mp-group** command to create an MP group interface or enter MP group interface view.

Use the **undo interface mp-group** command to remove an MP-group interface.

This command need to be used in conjunction with the **ppp mp mp-group** command. You can execute the two commands regardless of the order in which they are executed.

Example # Create MP group 3 interface.

```
<Sysname> system-view
[Sysname] interface mp-group 3
[Sysname-Mp-group3]
```

interface virtual-template

Syntax **interface virtual-ethernet** *number*

undo interface virtual-ethernet *number*

View System view

Parameter *number*: VT number, ranging from 0 to 1023.

Description Use the **interface virtual-template** command to create a VT or enter VT view.

Use the **undo interface virtual-template** command to remove a VT.

To remove a VT, make sure that all the relevant VA interfaces are removed and the VT is not being used.

Example # Create VT 10 interface.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10]
```

ip address ppp-negotiate

Syntax **ip address ppp-negotiate**

undo ip address ppp-negotiate

View Interface view

Parameter None

Description Use the **ip address ppp-negotiate** command to enable IP address negotiation on the local interface, so that the local interface can accept the IP address allocated by the remote end.

Use the **undo ip address ppp-negotiate** command to disable IP address negotiation.

By default, IP address negotiation is disabled.

Related command: **remote address**, **ppp ipcp remote-address forced**.

Example # Configure the IP address of interface Serial 1/0 to be negotiable.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ip address ppp-negotiate
```

link-protocol ppp

Syntax **link-protocol ppp**

View Interface view

Parameter None

Description Use the **link-protocol ppp** command to configure the link-layer protocol encapsulated on the interface as PPP.

By default, all interfaces except the Ethernet interface are encapsulated with PPP.

Example # Configure interface Serial 1/0 to encapsulate PPP.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] link-protocol ppp
```

ppp account-statistics enable

Syntax **ppp account-statistics enable**

undo ppp account-statistics enable

View Interface view

Parameters None

Description Use the **ppp account-statistics enable** command to enable the PPP accounting statistics function.

Use the **undo ppp account-statistics enable** command to disable the PPP accounting statistics function.

By default, the PPP accounting statistics function is disabled.

Examples # Enable the PPP accounting statistics function on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp account-statistics enable
```

ppp authentication-mode

Syntax **ppp authentication-mode** { **chap** | **pap** } [[**call-in**] **domain** *isp-name*]

undo ppp authentication-mode

View Interface view

Parameter **chap**, **pap**: Authentication modes. Use either mode.

call-in: Performs authentication only when receives a call from the remote end.

domain *isp-name*: Domain name during authentication, a string of 1 to 24 characters.

Description Use the **ppp authentication-mode** command to configure the PPP authentication mode used when the local device authenticates the peer.

Use the **undo ppp authentication-mode** command to disable authentication.

If you configure the **ppp authentication-mode** { **chap** | **pap** } command without specifying the **domain**, the default domain named system is used by default. Local authentication will be adopted and the address pool for address allocation must be the one you have configured for this domain.

If the **domain** is specified, you must configure an address pool in the specified domain.

If the username received includes a domain name, this domain name will be used for authentication (if the name does not exist, authentication is denied). Otherwise, the domain name configured for PPP authentication will be used.

If the username does not include a domain name, and the domain name configured for PPP authentication does not exist, authentication is denied.

By default, PPP authentication is not performed.

There are two types of PPP authentication: PAP and CHAP.

- PAP is a two-way handshake authentication, using plain text password.
- CHAP is a three-way handshake authentication, using ciphertext password.

In addition, you can also adopt the AAA authentication algorithm list (if defined) to perform authentication.

CHAP or PAP is just an authentication process. It is AAA that decides whether the authentication is successful or not. AAA uses a local authentication database or a AAA server to perform authentication.

For detailed description on how to create a local user and configure its attributes, and on how to create a domain and configure its attributes, refer to "local-user" on page 1940 and "domain" on page 1936.

For authentication on a dial-up interface, you are recommended to configure authentication on both the physical interface and the dialer interface. When the physical interface receives a DCC call request, it first initiates PPP negotiation and authenticates the dial-in user, and then passes the call to the upper layer protocol.

Related command: **local-user** on page 1940, **ppp chap user**, **ppp pap local-user**, ppp pap password, and **ppp chap password**.

Example # Authenticate the peer device by means of PAP on interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp authentication-mode pap domain system
```

ppp chap password

Syntax **ppp chap password** { **cipher** | **simple** } *password*

undo ppp chap password

View Interface view

Parameter **cipher**: Indicates to display the password in ciphertext.

simple: Indicates to display the password in plain text.

password: Default CHAP password, a string of 1 to 16 characters. When the **simple** keyword is used, this password is in plain text. When the **cipher** keyword is used, this password can either be in ciphertext or in plain text. The plain text is a string of no more than 16 characters, like aabbcc. The ciphertext has a fixed length of 24 characters, like _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description Use the **ppp chap password** command to configure the password for CHAP authentication.

Use the **undo ppp chap password** command to cancel the configuration.

Related command: **ppp authentication-mode chap**.

Example # Set the username to Sysname, which is to be displayed in plain text in CHAP authentication.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp chap password simple sysname
```

ppp chap user

Syntax **ppp chap user** *username*

undo ppp chap user

View Interface view

Parameter *username:* Username of CHAP authentication, a string of 1 to 80 characters, which is the one sent to the peer device to be authenticated.

Description Use the **ppp chap user** command to configure the user name when performing CHAP authentication.

Use the **undo ppp chap user** command to delete the existing configuration.

By default, the user name of the CHAP authentication is blank.

While configuring CHAP authentication, you should configure the *username* of both ends as the *local-user* of its peer, and configure the *password* accordingly.

Related command: **ppp authentication-mode**.

Example # On interface Serial 1/0, configure the local username as Root when performing CHAP authentication

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp chap user Root
```

ppp ipcp dns

Syntax **ppp ipcp dns** *primary-dns-address* [*secondary-dns-address*]

undo ppp ipcp dns *primary-dns-address* [*secondary-dns-address*]

View Interface view

Parameter *primary-dns-address*: IP address of the primary DNS server.

secondary-dns-address: IP address of the secondary DNS server.

Description Use the **ppp ipcp dns** command to set the device to allocate DNS server address for the peer.

Use the **undo ppp ipcp dns** command to disable the device to allocate DNS server address for the peer.

By default, the device does not allocate DNS server addresses for its peer.

When connected using PPP, a device can assign a DNS server address to its peer after negotiation (usually based on the request of the peer), allowing the peer to access the network directly using domain name.

If a PC is connected to the device using PPP, you can use the **winipcfg** command or the **ipconfig/all** command to view its DNS server address assigned by the device.

A sysname device can provide a primary DNS server address and a secondary DNS server address.

Example # Configure the local device to assign primary DNS server address 100.1.1.1, and secondary DNS server address 100.1.1.2 to its peer.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp ipcp dns 100.1.1.1 100.1.1.2
```

ppp ipcp dns admit-any

Syntax **ppp ipcp dns admit-any**

undo ppp ipcp dns admit-any

View Interface view

Parameter None

Description Use the **ppp ipcp dns admit-any** command to configure the device to passively accept the DNS server address assigned by the peer, even without sending a DNS request.

Use the **undo ppp ipcp dns admit-any** command to disable this function.

By default, a device does not passively accept DNS server address assigned by the peer.

When a device is connected to another device (for example, a network access server of a service provider) using PPP, the device can be configured to accept the DNS server address allocated by the peer to resolute the domain name.

Example # Set the interface Serial 1/0 of the local device to accept DNS server address allocated by the peer.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp ipcp dns admit-any
```

ppp ipcp dns request

Syntax **ppp ipcp dns request**

undo ppp ipcp dns request

View Interface view

Parameter None

Description Use the **ppp ipcp dns request** command to enable a device to request its peer for the DNS server address actively through a port.

Use the **undo ppp ipcp dns request** command to restore the default.

By default, a device does not request its peer for the DNS server address actively.

You can configure a device to request its peer (especially in cases where a device is connected to the operator's access server through a dialup link) for the DNS server address during PPP negotiation, after which domain names can be resolved on the device.

You can check the DNS server address of a port by displaying the information about the port.

Example # Enable the device to request its peer for the DNS server address actively through Serial 2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp ipcp dns request
```

ppp ipcp remote-address forced

Syntax **ppp ipcp remote-address forced**

undo ppp ipcp remote-address forced

View Interface view

Parameter None

Description Use the **ppp ipcp remote-address forced** command to forbid the peer to use self-configured IP address, but have to use the one allocated by the local device.

Use the **undo ppp ipcp remote-address forced** command to cancel this feature.

By default, the peer can use its self-configured IP address in PPP IPCP negotiation. The peer can request the local device for an address or use a fixed IP address configured by itself

If you do not want the peer to use self-configured IP address, you must configure the **ppp ipcp remote-address forced** command on the local interface.

Related command: **remote address**.

Example # Configure the interface serial 1/0 to allocate the IP address 10.0.0.1 to the peer. The peer may accept this assigned address, or use its self-configured address, or have no IP address.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] remote address 10.0.0.1
```

Configure the interface serial 1/0 to allocate the IP address 10.0.0.1 to the peer. The peer must accept this allocated address and cannot use its self-configured address or go without IP address.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] remote address 10.0.0.1
[Sysname-Serial1/0] ppp ipcp remote-address forced
```

ppp lqc

Syntax **ppp lqc** *close-percentage* [*resume-percentage*]

undo ppp lqc

View Interface view

Parameter *close-percentage*: If the link quality decreases below this percentage, the link will go down. The value ranges from 0 to 100.

resume-percentage: If the link quality recovers above this percentage, the link will go up. The value ranges from 0 to 100.

Description Use the **ppp lqc** command to enable PPP link quality control (LQC).

Use the **undo ppp lqc** command to disable PPP link quality control.

By default, PPP LQC is disabled.

By default, the arguments *resume-percentage* and *close-percentage* are equal. But in actual configuration, the *resume-percentage* must not be smaller than *close-percentage*.

PPP LQC functions to monitor the quality of PPP links, including those in MP bundles. A link goes down when its quality drops below the close percentage and goes up when its quality exceeds the resume-percentage. To avoid flapping, a link experiences a delay before it is reused.

Before you enable PPP LQC, the PPP interface sends keepalives to the peer every some time. After you enable LQC on the interface, it sends link quality reports (LQRs) instead of keepalives to monitor the link.

When link quality is normal, the system calculates link quality based on each LQR and disables the link if the results of two consecutive calculations are below the close-percentage. Once the link is disabled, the system starts to calculate link

quality every ten LQRs, and brings the link up if the results of three consecutive calculations are higher than the resume-percentage. This means a disabled link must experience 30 keepalive periods before it can go up again. If a large keepalive period is specified, it may take long time for the link to go up.

When enabling LQC at both ends of a PPP link, you must set the same parameters on the devices involved. Normally, it is not recommended to enable LQC at both ends of a link. In addition, LQC on dial-up line is not recommended too. This is because that when a link on dial-up line is disabled, the DCC would disconnect the dial-up line, causing LQC not to work. It is not until there are data to transmit, will DDC brings the dial-up line up again and LQC resumes to work.

Example # Enable LQC on interface Serial 1/0, setting close-percentage to 90 and resume-percentage to 95.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp lqc 90 95
```

ppp mp

Syntax **ppp mp**

undo ppp mp

View Interface view

Parameter None

Description Use the **ppp mp** command to enable MP on the interface encapsulated with PPP.

Use the **undo ppp mp** command to disable this feature.

By default, the interface encapsulated with PPP operates in the Single PPP mode.

To increase bandwidth, multiple PPP links can be bound to form a logical MP interface.

Example # Configure the PPP encapsulated interface Serial 1/0 to work in MP mode.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp mp
```

ppp mp binding-mode

Syntax **ppp mp binding-mode** { **authentication** | **both** | **descriptor** }

undo ppp mp binding-mode

View Virtual template interface view, dialer interface view

Parameter **authentication**: Performs MP binding according to PPP authentication username.

both: Performs MP binding according to both the PPP authentication username and the endpoint descriptor.

descriptor: Performs the MP binding according to the endpoint descriptor.

Description Use the **ppp mp binding-mode** command to set the MP binding mode.

Use the **undo ppp mp binding-mode** command to restore the default MP binding mode.

By default, MP binding is based on both the PPP authentication username and the endpoint descriptor.

The username is the peer's username received while performing PAP or CHAP authentication. The endpoint descriptor, which uniquely specifies a device, refers to the peer's endpoint descriptor received when performing LCP negotiation. Based on the username or endpoint descriptor, the system can locate the specified VT interface and create a MP binding according to the configuration on the template.

Note that:

- When MP binding is only based on descriptors, users cannot be differentiated. So, to bind users to different groups, use the keyword **both** in the command.
- When MP binding is only based on authentication usernames, peer devices cannot be differentiated. So, when multiple peer devices exist, use the keyword **both** in the command.

Related command: **ppp mp user**.

Example # Perform MP binding based on PPP authentication username.

```
<Sysname> system-view
[Sysname] interface dialer 0
[Sysname-Dialer0] ppp mp binding-mode authentication
```

ppp mp max-bind

Syntax **ppp mp max-bind** *max-bind-num*

undo ppp mp max-bind

View Virtual template interface view, dialer interface view

Parameter *max-bind-num*: Specifies the maximum number of links which can be bound, in the range 1 to 128.

Description Use the **ppp mp max-bind** command to configure the maximum number of links allowed in an MP bundle.

Use the **undo ppp mp max-bind** command to restore the default value, which is 16.

Generally speaking, it is unnecessary to configure this argument, but in case you need to configure it, you must do it under the guidance of technical engineers. Such a configuration may affect the performance of PPP.

- *If MP fails to delete links, it is possibly because that the maximum number of bundled links is smaller than what has actually been configured. Make sure that the maximum binding number is larger than the actual one.*
- *After you change the maximum number of bundled links in an MP on a virtual-template or dialer interface, you must **shutdown** and then **undo shutdown** the relevant physical interfaces before modification takes effect.*

Related command: **ppp mp**.

Example # Set the maximum number of binding links to 12.

```
<Sysname> system-view
[Sysname] interface virtual-template 0
[Sysname-Virtual-Template0] ppp mp max-bind 12
```

ppp mp min-bind

Syntax **ppp mp min-bind** *min-bind-num*

undo ppp mp min-bind

View Dialer interface view

Parameter *min-bind-num*: Specifies the minimum number of links in an MP bundle, in the range 1 to 128.

Description Use the **ppp mp min-bind** command to configure the minimum number of PPP links that an MP bundle should contain.

Use the **undo ppp mp min-bind** command to restore the default value.

By default, the minimum number of PPP links in an MP bundle is 0, which means that MP dial-up relies on traffic detection.

In dial-up application, you sometimes need multiple links to bear services simultaneously to guarantee the minimum bandwidth in transmitting a packet. In this case, you can use this command to set the minimum links to be bound.

Note that, after you configure the **ppp mp min-bind** command, MP dial-up no longer depends on traffic detection. Moreover, links that have been established will not be removed even in case of timeout. This means that after the **ppp mp**

min-bind command is configured, the **dialer timer idle** command no longer takes effect.

The argument *min-bind-num* must be no greater than *max-bind-num*.

Related command: **dialer threshold** on page 324

Example # Set the minimum number of links contained in an MP bundle to 4.

```
<Sysname> system-view
[Sysname] interface dialer 0
[Sysname-dialer0] ppp mp min-bind 4
```

ppp mp min-fragment

Syntax **ppp mp min-fragment** *size*

undo ppp mp min-fragment

View Virtual template interface view, dialer interface view, MP-group interface view

Parameter *size*: Specifies the minimum MP outgoing packet size to be fragmented, in bytes. The value ranges from 128 to 1500. If the MP outgoing packet is smaller than this value, it will not be fragmented. If the MP packet is larger than or equal to this value, it will be fragmented.

Description Use the **ppp mp min-fragment** command to set the minimum size of MP outgoing packet to be fragmented.

Use the **undo ppp mp min-fragment** command to restore the default, that is, 128 bytes.

If you do not want small packets to be fragmented, you can specify the *size* argument to an appropriate value.

- *If MP bundle is implemented through hardware (CPOS chip for example), the minimum fragment size varies with chips (for example, the fragment size on certain chips can only be 128, 256, and 512 bytes). In this case, you need to make sure the setting specified by the **ppp mp min-fragment** command conforms to the hardware specification for the MP bundle and the sub-channel LCP link to be established successfully.*
- *After executing the **ppp mp min-fragment** command, you need to shut down and then bring up all the bundled ports for the new setting to take effect.*

Example # Set the minimum MP packet size for fragmentation to 500 bytes.

```
<Sysname> system-view
[Sysname] interface virtual-template 0
[Sysname-Virtual-Template0] ppp mp min-fragment 500
```

ppp mp mp-group

Syntax **ppp mp mp-group** *number*

undo ppp mp

View Interface view

Parameter *number*: MP-group interface number, in the range 0 to 1023.

Description Use the **ppp mp mp-group** command to add the current interface to the specified MP-group.

Use the **undo ppp mp mp-group** command to remove the current interface from the specified MP-group.

This command should be used along with the **interface mp-group** command. With the two commands, you can create an MP-group interface first and then add an interface to the MP-group. It does not matter if you reverse the two steps.

Note that only physical interfaces can be added to an MP group. Logical interfaces such as Tunnel interfaces do not support this command.

Example # Add interface Serial 3/0 to MP-group 3.

```
<Sysname> system-view
[Sysname] interface serial 3/0
[Sysname-Serial3/0] ppp mp mp-group 3
```

ppp mp user

Syntax **ppp mp user** *username* **bind virtual-template** *number*

undo ppp mp user *username*

View System view

Parameter *username:* User name, a string of 1 to 80 characters.

virtual-template *number*: Specifies a virtual-template. The *number* argument is in the range of 0 to 1023.

Description Use the **ppp mp user** command to bind an MP user to a virtual template.

Use the **undo ppp mp user** command to remove the specified binding.

In establishing a PPP connection, after PPP authentication succeeds, if a virtual-template is specified, MP will be bound based on the parameters of the virtual-template and a new virtual interface will be formed to transfer data.

You can configure the following parameters on the virtual-template:

- Local IP address and the IP address (or IP address pool) assigned to the peer
- PPP working parameter

Related command: **ppp mp** and **ppp mp max-bind**.

Example # Specify the VT interface that corresponds to user 1 as 1, and configure the IP address of the VT as 202.38.60.1.

```
<Sysname> system-view
[Sysname] ppp mp user user1 bind virtual-template 1
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ip address 202.38.60.1 255.255.255.0
```

ppp mp virtual-template

Syntax **ppp mp virtual-template** *number*

undo ppp mp

View Interface view

Parameter *number:* Specifies the VT interface number to be bound on the interface, in the range 0 to 1023.

Description Use the **ppp mp virtual-template** command to configure the VT interface number to be bound on the interface, enabling the interface to work in MP mode.

Use the **undo ppp mp** command to remove MP binding of the interface, making the interface to work in PPP mode.

By default, MP binding on the interface is disabled, and the interface works in PPP mode.

This command specifies the VT interface number to be bound on the interface. In configuring MP binding on the interface configured with this command, you needs not configure PAP or CHAP authentication.

Two or more interfaces with the same virtual template number is bound directly together. Moreover, once you used this command on an interface, you cannot use the **ppp mp** command on the same interface, and vice versa.

Example # Configure interface serial 1/0 encapsulated with PPP to work in MP mode, with the VT interface being Virtual-Template1

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp mp virtual-template 1
```

ppp pap local-user

Syntax **ppp pap local-user** *username* **password** { **cipher** | **simple** } *password*

undo ppp pap local-user

View Interface view

Parameter *username*: Specifies the username sent by the local device when it is authenticated by the peer device via PAP, a string of 1 to 80 characters.

cipher: Displays the password in ciphertext.

simple: Displays the password in plain text.

password: Specifies the password sent by the local device when it is authenticated by the peer device using PAP, a string of 1 to 16 characters. When the **simple** keyword is used, this password is in plain text. When the **cipher** keyword is used, this password can be either in ciphertext or plain text. The plain text is a string of no more than 16 characters, like aabbcc. The ciphertext has a fixed length of 24 characters, like _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description Use the **ppp pap local-user** command to configure the username and password sent by the local device when it is authenticated by the peer device via the PAP method.

Use the **undo ppp pap local-user** command to disable the configuration.

By default, both the username and the password are empty.

When the local router is authenticated via the PAP method by the peer device, the *username* and *password* sent by the local device must be the same as the *username* and *password* of the peer router.

Related command: **local-user** on page 1940, **password** on page 1941

Example # Set the username of the local device authenticated by the peer via PAP as user1 and the password as pass1.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp pap local-user user1 password simple pass1
```

ppp timer negotiate

Syntax **ppp timer negotiate** *seconds*

undo ppp timer negotiate

View Interface view

Parameter *seconds:* Period of negotiation timeout in seconds. In PPP negotiation, if the local device fails to receive a response from the peer during this period of time, PPP will resend the last packet. This period ranges from 1 to 10 seconds.

Description Use the **ppp timer negotiate** command to set the PPP negotiation timeout interval.

Use the **undo ppp timer negotiate** command to restore the default value.

By default, the PPP negotiation timeout interval is three seconds.

Example # Set the PPP negotiation timeout interval to five seconds.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp timer negotiate 5
```

remote address

Syntax **remote address** { *ip-address* | **pool** [*pool-number*] }

undo remote address

View Interface view

Parameter *ip-address*: Indicates the IP address assigned to the peer.

pool [*pool-number*]: Specifies an address pool identified by the *pool-number* argument. An IP address from this address pool will be assigned to the peer. The *pool-number* argument ranges from 0 to 99 and defaults to 0.

Description Use the **remote address** command to allocate IP address for the peer device.

Use **undo remote address** to remove the IP address allocated for the peer device.

By default, an interface does not allocate IP address for the peer device. If the *pool-numbe*r argument is not specified while using this command, the global address pool 0 will be used by default.

This command can be used in situation when the local device is configured with an IP address, while the peer has no IP address. To accomplish the configuration, you need to configure the **ip address ppp-negotiate** command on the peer device, and configure the **remote address** command on the local device, so that the peer device can accept IP address allocated to it through PPP negotiation.

CAUTION: *This command allows the peer device to configure its IP address by itself even if it has received an IP address allocated by the local device. If you do not want this to happen, you must configure the* ***ppp ipcp remote-address forced*** *command to forbid the peer device to configure its own IP address.*

Related command: **ip address ppp-negotiate**, **ppp ipcp remote-address forced**

Example # Configure Interface Serial 1/0 to allocate IP address 10.0.0.1 to its peer device.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] remote address 10.0.0.1
```

timer hold

Syntax **timer hold** *seconds*

undo timer hold

View Interface view

Parameter *seconds:* Time interval for the interface to send keepalive packet in seconds. The value ranges from 0 to 32767 and defaults to 10. If the value is set to 0, keepalive packet will not be sent.

Description Use the **timer hold** command to set the timer to send keepalive packet.

Use the **undo timer hold** command to restore the default value, or 10 seconds.

If the timer is set to 0 seconds, this means keepalive packets will not be sent out.

On slow links, the *seconds* argument must not be too small. As a slow link takes long to transmit large packets, this may cause the sending and receiving of keepalive packet to be postponed. If an interface does not receive keepalive packet from the peer device for many keepalive periods, it regards the link to be bad. If this period exceeds the value specified by the *seconds* argument, the link will be shut down.

When the interfaces are configured with PPP, the same keepalive interval should be configured on both sides of the link.

Example # Set the period to send keepalive packet on interface Serial 1/0 to 20 seconds.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] timer hold 20
```

32 PPP LINK EFFICIENCY MECHANISM CONFIGURATION COMMANDS

display ppp compression iphc rtp

Syntax **display ppp compression iphc rtp** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ppp compression iphc rtp** command to view statistics about IPHC RTP header compression.

Note that:

- When IPHC RTP header compression is applied on an MP link, the compression is performed on the VA (virtual access) interfaces. In this case, you can check the compression information on MP templates, such as VT or Dialer.
- When IPHC RTP header compression is applied on a normal PPP link, the compression is performed on the physical link. In this case, you can check the compression information on the physical interfaces only.

Example # Display statistics about IPHC RTP header compression.

```
<Sysname> display ppp compression iphc rtp
```

display ppp compression iphc tcp

Syntax **display ppp compression iphc tcp** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ppp compression iphc tcp** command to display statistics about IPHC TCP header compression.

Note that:

- When IPHC TCP header compression is applied on an MP link, the compression is performed on the VA (virtual access) interfaces. In this case, you can check the compression information on MP templates, such as VT or Dialer.
- When IPHC TCP header compression is applied on a normal PPP link, the compression is performed on the physical link. In this case, you can check the compression information on the physical interfaces only.

Example # Display statistics about IPHC TCP header compression.

```
<Sysname> display ppp compression iphc tcp
```

display ppp compression stac-lzs

Syntax **display ppp compression stac-lzs** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ppp compression stac-lzs** command to view statistics about STAC-LZS compression.

Note that:

- When STAC-LZS header compression is applied on an MP link, the compression is performed on the VA (virtual access) interfaces. In this case, you can check the compression information on MP templates, such as VT or Dialer.
- When STAC-LZS compression is applied on a normal PPP link, the compression is performed on the physical link. In this case, you can check the compression information on the physical interfaces only.

Example # Display information about STAC-LZS compression.

```
<Sysname> display ppp compression stac-lzs
Staz-lzs compression
  Interface: Serial1/1:0
    Received:
      Compress/Error/Discard/Total: 302/0/0/302 (Packets)
    Sent:
      Compress/Error/Total: 302/0/302 (Packets)
```

ip tcp vjcompress

Syntax **ip tcp vjcompress**

undo ip tcp vjcompress

View Interface view

Parameter None

Description Use the **ip tcp vjcompress** command to enable a PPP interface to compress the VJ TCP header.

Use the **undo ip tcp vjcompress** command to disable the PPP interface to compress the VJ TCP header.

By default, the VJ TCP header compression is disabled on PPP interfaces.

If a PPP interface is enabled to perform VJ TCP header compression, so should the interface at the opposite end.

Example # Enable VJ TCP header compression on interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ip tcp vjcompress
```

ppp compression iphc

Syntax **ppp compression iphc** [**nonstandard**]

undo ppp compression iphc

View Interface view

Parameter **nonstandard**: Nonstandard encapsulation mode.

Description Use the **ppp compression iphc** command to enable IP header (TCP header and RTP header mainly) compression on the interface.

Use the **undo ppp compression iphc** command to disable IP header compression.

By default, TCP header compression and RTP header compression are disabled.

Once IP header compression is enabled, the header compression for TCP packets used to establish RTP sessions is also enabled. When IP header compression is disabled, the header compression for TCP packets used to establish RTP sessions is also disabled.

To enable IP header compression, you need to execute the **ppp compression iphc** command on both ends of the link.

Note that:

- If the configuration is applied on VT and Dialer interfaces, ISDN and asynchronous dialer interfaces, the configuration takes effect only after you shutdown and then bring up the interfaces.

- If the configuration is applied on a MP bundle, you need to shut down and then bring up all the member interfaces of the MP bundle for the configuration to take effect.

Related command: **ppp compression iphc rtp-connections**, **ppp compression iphc tcp-connections**.

Example # Enable IP header compression on interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp compression iphc
```

ppp compression iphc rtp-connections

Syntax **ppp compression iphc rtp-connections** *number*

undo ppp compression iphc rtp-connections

View Interface view

Parameter *number*: The maximum connection number of RTP header compression. The value ranges from 3 to 1000.

Description Use the **ppp compression iphc rtp-connections** command to specify the maximum number of RTP header compression connections allowed on an interface.

Use the **undo ppp compression iphc rtp-connections** command to restore the default value, which is 16.

RTP is connection oriented; the number of RTP connections that a link can accommodate is relatively large. The compression algorithm, however, requires the device to maintain some information for each connection when compressing headers. To restrict the memory load generated by compression, you can use the **ppp compression iphc rtp-connections** command to limit the number of compression. For example, if you limit RTP connections to three, the packets on the fourth RTP connection will not be compressed.

The configuration takes effect after you execute the command **shutdown** and then **undo shutdown** on the interface. If you are configuring MP, you must execute the commands **shutdown** and **undo shutdown** on all MP member interfaces.

Example # Set the number of compression-enabled RTP header connections to 10 on interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp compression iphc rtp-connections 10
```

ppp compression iphc tcp-connections

Syntax **ppp compression iphc tcp-connections** *number*

undo ppp compression iphc tcp-connections

View Interface view

Parameter *number*: The maximum connection number of TCP header compression. The value ranges from 3 to 256.

Description Use the **ppp compression iphc tcp-connections** command to configure the maximum number of connections in TCP header compression.

Use the **undo ppp compression iphc tcp-connections** command to restore the default value, which is 16.

TCP is connection oriented; the number of TCP connections that a link can accommodate is relatively large. The use of compression however requires the router to maintain some information for each connection when compressing headers. To restrict the memory load generated by compression, you can use the **ppp compression iphc tcp-connections** command to limit the number of compression-enabled TCP connections to three for example. The packets on the fourth TCP connection are not compressed as a result.

The configuration takes effect only after you perform the **shutdown** and then the **undo shutdown** operations on the interface. If the configuration is for an MP bundle, you should perform the operations on all MP member interfaces.

Example # Set the number of compression-enabled TCP connections to 10 on interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] ppp compression iphc tcp-connections 10
```

ppp compression stac-lzs

Syntax **ppp compression stac-lzs**

undo ppp compression stac-lzs

View Interface view

Parameter None

Description Use the **ppp compression stac-lzs** command to enable STAC-LZS compression for PPP.

Use the **undo ppp compression stac-lzs** command to disable STAC-LZS compression on the current interface.

By default, this compression is disabled.

STAC-LZS compression is supported on the current version of system. You can configure STAC-LZS compression on an interface to reduce size of data frames through lossless compression. However, as this can increase the load on the device, you are recommended to disable the function when the device is heavily loaded.

Note that STAC-LZS compression takes effect on a PPP link only when the **stac-lzs** option is configured on both ends of the link. Currently, outbound expedite forwarding is not applicable on links with Stac-LZS compression enabled. So, it is recommended that you disable outbound fast forwarding before execute the **ppp compression stac-lzs** command.

Note that:

- If the configuration is applied on VT and Dialer interfaces, ISDN and asynchronous dialer interfaces, the configuration takes effect only after you shut down and then bring up the interfaces.
- If the configuration is applied on a MP bundle, you need to shut down and then bring up all the member interfaces of the MP bundle for the configuration to take effect.

Example # Enable STAC-LZS compression on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ppp compression stac-lzs
```

ppp mp lfi

Syntax **ppp mp lfi**

undo ppp mp lfi

View Virtual template interface view, MP-group interface view, dialer interface view

Parameter None

Description Use the **ppp mp lfi** command to enable link fragmentation and interleaving (LFI) on the interface.

Use the **undo ppp mp lfi** command to disable the function.

By default, LFI is disabled.

Example # Enable LFI on Virtual-Template1.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp mp lfi
```

ppp mp lfi delay-per-frag

Syntax **ppp mp lfi delay-per-frag** *time*

undo ppp mp lfi delay-per-frag

View Virtual template interface view, MP-group interface view, dialer interface view

Parameter *time*: Maximum time delay of LFI fragment in ms, in the range 1 to 1000.

Description Use the **ppp mp lfi delay-per-frag** command to set the maximum time delay for transmitting a LFI fragment.

Use the **undo ppp mp lfi delay-per-frag** command to restore the default value, or 10 ms.

Example # Set the maximum time delay of LFI fragment of Virtual-Template1 to 20 ms.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] ppp mp lfi delay-per-frag 20
```

reset ppp compression iphc

Syntax **reset ppp compression iphc** [*interface-type interface-number*]

View User view

Parameter *Interface-type Interface-number:* Specifies an Interface by its type and number.

Description Use the **reset ppp compression iphc** command to delete IP header compression statistics.

If the *interface-type* and *interface-number* arguments are not specified, the IP header compression statistics on all interfaces will be cleared.

Example # Reset statistics about IP header compression on all interfaces.

```
<Sysname> reset ppp compression iphc
```

33 PPPoE Server Configuration Commands

display pppoe-server session

Syntax **display pppoe-server session { all | packet }**

View Any view

Parameter **all**: Displays all information about each PPPoE session.

packet: Displays statistics about the packets on each PPPoE session.

Description Use the **display pppoe-server session** command to view the status and statistics of PPPoE session.

*The support for the **display pppoe-server session packet** command varies with device models.*

Example # View all the session information of PPPoE.

```
<Sysname> display pppoe-server session all
SID Intf                 State  OIntf          RemMAC          LocMAC
2   Virtual-Template1:0  UP  Ethernet1/0  0050.ba22.7369  00e0.fc08.f4de
```

Table 84 Description on the fields of the display pppoe-server session all command

Field	Description
SID	PPPoE session identifier
Intf	The corresponding Virtual-Template interface
State	State PPPoE of sessions
OIntf	corresponding Ethernet interface
RemMAC	Remote MAC address
LocMAC	Local MAC address

View the statistics of PPPoE session.

```
Sysname> display pppoe-server session packet
SID   RemMAC    LocMAC        InP     InO   InD     OutP     OutO  OutD
1  0050ba1a02ce 0001af02a40f  42      2980  0       16       343   0
```

Table 85 Description on the fields of the display pppoe-server session packet command

Field	Description
SID	PPPoE session identifier
RemMAC	Remote MAC address
LocMAC	Local MAC address

Table 85 Description on the fields of the display pppoe-server session packet command

Field	Description
InP	In Packets, Packages received
InO	In Octets, Bytes received
InD	In Discards, Received and then discarded packages
OutP	Out Packets, Packages sent
OutO	Out Octets, Bytes sent
OutD	Out Discard, Discarded packages that might be sent

pppoe-server bind

Syntax **pppoe-server bind virtual-template** *number*

undo pppoe-server bind

View Interface view

Parameter *number*: Number of the virtual-template interface, in the range 0 to 1023.

Description Use the **pppoe-server bind** command to enable PPPoE on the virtual-template specified by the Ethernet interface.

Use the **undo pppoe-server bind** command to disable PPPoE protocol on the relevant interface.

By default, PPPoE protocol is disabled.

Example # Enable PPPoE on interface Ethernet 1/0, and bind Virtual-Template1 with interface Ethernet 1/0

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pppoe-server bind virtual-template 1
```

pppoe-server log-information off

Syntax **pppoe-server log-information off**

undo pppoe-server log-information off

View System view

Parameter None

Description Use the **pppoe-server log-information off** command to disable the PPPoE server to display the PPP log information.

Use the **undo pppoe-server log-information off** command to enable the function.

By default, the PPPoE server displays the PPP log information.

Displaying too much log information can affect the performance of the device and can be a nuisance to user during configuration. You can use this command to disable the PPPoE server to display the PPP log information.

Example # Disable the PPPoE server to display PPP log information.

```
<Sysname> system-view
[Sysname] pppoe-server log-information off
```

pppoe-server max-sessions local-mac

Syntax **pppoe-server max-sessions local-mac** *number*

undo pppoe-server max-sessions local-mac

View System view

Parameter *number:* Maximum number of sessions that can be established at a local MAC address, in the range 1 to 4069.

Description Use the **pppoe-server max-sessions local-mac** command to set the maximum number of PPPoE sessions that can be established at a local MAC address.

Use the **undo pppoe-server max-sessions local-mac** command to restore the default configuration.

By default, the value of *number* is 100.

Example # Set the maximum number of PPPoE sessions that can be established at a local MAC address to 50.

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions local-mac 50
```

pppoe-server max-sessions remote-mac

Syntax **pppoe-server max-sessions remote-mac** *number*

undo pppoe-server max-sessions remote-mac

View System view

Parameter *number*: Maximum number of PPPoE sessions that can be established by the system with regard to a peer MAC address, in the range 1 to 4096.

Description Use the **pppoe-server max-sessions remote-mac** command to set the maximum number of PPPoE sessions that can be established by the system with regard to a peer MAC address.

Use the **undo pppoe-server max-sessions remote-mac** command to restore the default configuration.

By default, the value of *number* is 100.

Example # Set the maximum number of PPPoE sessions that can be established by the system with regard to a peer MAC address to 50.

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions remote-mac 50
```

pppoe-server max-sessions total

Syntax **pppoe-server max-sessions total** *number*

undo pppoe-server max-sessions total

View System view

Parameter *number*: Maximum number of PPPoE sessions that the system can establish, which ranges from 1 to 65535.

Description Use the **pppoe-server max-sessions total** command to set the maximum number of PPPoE sessions that the system can establish.

Use the **undo pppoe-server max-sessions total** command to restore the default configuration.

By default, the value of *number* is 4096.

Example # Set the maximum number of PPPoE sessions established by the system to 3000.

```
<Sysname> system-view
[Sysname] pppoe-server max-sessions total 3000
```

reset pppoe-server

Syntax **reset pppoe-server** { **all** | **interface** *interface-type interface-number* | **virtual-template** *number* }

View User view

Parameter **all**: Terminates all the PPPoE sessions.

interface *interface-type interface-number*: Specifies an interface by its type and number.

virtual-template *number*: Specifies a virtual template interface.

Description Use the **reset pppoe-server** command to terminate a PPPoE session on the server side.

Example # Terminate the session established on virtual template interface 1 on the server side.

```
<Sysname> reset pppoe-server virtual-template 1
```

34 PPPoE Client Configuration Commands

display pppoe-client session

Syntax **display pppoe-client session** { **packet** | **summary** } [**dial-bundle-number** *number*]

View Any view

Parameter **packet**: Displays the statistics of PPPoE session data packet.

summary: Displays the summary of PPPoE session.

dial-bundle-number *number*: Displays the statistics of the specified PPPoE session, in the range 1 to 255. If PPPoE session is not specified, the system will display the statistics of all PPPoE sessions.

Description Use the **display pppoe-client session** command to display the state and statistics of PPPoE session.

Example # Display the summary of PPPoE session.

```
<Sysname> display pppoe-client session summary
There are 2 sessions in total:
ID   Bundle  Dialer  Intf          Client-MAC    Server-MAC    State
1     1        1     Eth1/0        00e0fc0254f3  00049a23b050  PPPUP
2     2        2     Eth1/0        00e0fc0254f3  00049a23b050  PPPUP
```

Table 86 Description on the fields of display pppoe-client session summary

Field	Description
ID	Session ID, PPPoE session ID
Server-MAC	MAC address of PPPoE server
Client-MAC	MAC address of PPPoE client
Dialer	Corresponding dialer interface of PPPoE session
Bundle	Dialer bundle containing PPPoE session
Intf	Ethernet interface containing PPPoE session
State	State of PPPoE session

Display the statistics of PPPoE session packet

```
<Sysname> display pppoe-client session packet
PPPoE Client Session:
ID    InP         InO         InD         OutP        OutO       OutD
================================================================
```

```
1       164         6126        0           83          1069        0
2       304         9886        0           156         2142        0
```

Table 87 Description on the fields of display pppoe-server session packet

Field	Description
ID	PPPoE session ID
InP	In Packets: number of received packets
InO	In Octets: number of received octets
InD	In Discards: number of illegal packets received and discarded
OutP	Out Packets: number of packets sent
OutO	Out Octets: number of octets sent
OutD	Out Discards: number of illegal packets sent and discarded

pppoe-client dial-bundle-number

Syntax **pppoe-client dial-bundle-number** *number* [**no-hostuniq**] [**idle-timeout** *seconds* [**queue-length** *packets*]]

undo pppoe-client dial-bundle-number *number*

View Ethernet interface view, virtual Ethernet interface view

Parameter **dial-bundle-number** *number*: Dialer bundle number corresponding to PPPoE session, in the range 1 to 255 The *number* argument can be used to uniquely specify a PPPoE session, or as a PPPoE session.

no-hostuniq: The call originated from PPPoE client does not carry the Host-Uniq field. By default, **no-hostuniq** is not configured.

idle-timeout *seconds*: Idle time of PPPoE session in seconds, its value ranges from 1 to 65535. If the parameter is not configured, PPPoE session will work in permanent online mode. Otherwise, it works in packet trigger mode.

queue-length *packets*: packet number cached in the system before PPPoE session is established, its value ranges from 1 to 100. Only after **idle-timeout** is configured will the parameter be enabled. By default, *packets* is 10.

Description Use the **pppoe-client** command to establish a PPPoE session and specify the dialer bundle corresponding to the session.

Use the **undo pppoe-client** command to delete a PPPoE session.

By default, no PPPoE session is configured.

An Ethernet interface can be configured with multiple PPPoE sessions, which means an Ethernet interface can belong to multiple dialer bundles. However, a dialer bundle can own only one Ethernet interface. Each PPPoE session correspond to one dialer bundle. If a dialer bundle at a certain dialer interface has had one Ethernet interface been used by PPPoE, other interfaces cannot be added to this dialer bundle. Likewise, if a dialer bundle has had interfaces other than the PPPoE

Ethernet interface, this dialer bundle can also not be added to the Ethernet interface used by PPPoE Client.

When PPPoE session works in permanent online mode, and the physical lines go UP, the device will immediately initiate PPPoE call to establish PPPoE session. This PPPoE connection will exist constantly unless users use the command **undo pppoe-client** to delete PPPoE session. When PPPoE session works in packet trigger mode, the device will not initiate PPPoE call to establish PPPoE session unless it has data to transmit. If there is no data transmission on the PPPoE link within *seconds*, the device will automatically terminate PPPoE session. Only after it has new data to transmit, PPPoE session will be re-established.

Related command: **reset pppoe-client**.

*The difference between the **reset pppoe-client** command and the undo pppoe-client command lies in: the former only temporarily terminates a PPPoE session, while the latter permanently deletes a PPPoE session.*

No matter a PPPoE session works in permanent on-line mode or in packet triggering mode, it will be deleted permanently by the undo pppoe-client command. If it is necessary to recreate a PPPoE session, the user must reconfigure it.

Example # Create a PPPoE session on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pppoe-client dial-bundle-number 1
```

reset pppoe-client

Syntax **reset pppoe-client** { **all** | **dial-bundle-number** *number* }

View User view

Parameter **all**: Clears all PPPoE sessions.

dial-bundle-number *number*: Dialer bundle number, in the range 1 to 255, which is used to clear the PPPoE session corresponding to dialer bundle.

Description Use the **reset pppoe-client** command to terminate PPPoE session and re-initiate the connection later.

When a PPPoE session works in permanent on-line mode, if it is terminated by the **reset pppoe-client** command, the device will automatically recreate a PPPoE session in 16 seconds. When a PPPoE session works in packet triggering mode, if it is terminated via the **reset pppoe-client** command, the device will recreate a PPPoE session only upon data transmission.

Related command: pppoe-client.

*The difference between the **reset pppoe-client** command and the undo pppoe-client command lies in: the former only temporarily terminates a PPPoE session, while the latter permanently deletes a PPPoE session.*

Example # Clear all PPPoE sessions, and re-initiate PPPoE session later.

```
<Sysname> reset pppoe-client all
```

35 PPP DEBUGGING COMMANDS

debugging ppp

Syntax **debugging ppp** { **all** [**interface** *interface-type interface-number*] | **bcp** | **cbcp packet** [**interface** *interface-type interface-number*] | **ccp** | **chap** | **compression iphc** { **rtp** | **tcp** } | **core event** [**interface** *interface-type interface-number*] | **ip packet** [**interface** *interface-type interface-number*] | **ipcp** | **ipv6** | **ipv6cp** | **ipx** | **ipxcp** | **lcp** | **lqc** | **mp** | **mpls-multicast packet** [**interface** *interface-type interface-number*] | **mpls-unicast packet** [**interface** *interface-type interface-number*] | **mplscp** | **osi-npdu** | **osicp** | **pap** | **scp** | **vjcomp** { **all** | **error** | **event** | **packet** | **state**} [**interface** *interface-type interface-number*] }

undo debugging ppp { **all** [**interface** *interface-type interface-number*] | **bcp** | **cbcp packet** [**interface** *interface-type interface-number*] | **ccp** | **chap** | **compression iphc** { **rtp** | **tcp** } | **core event** [**interface** *interface-type interface-number*] | **ip packet** [**interface** *interface-type interface-number*] | **ipcp** | **ipv6** | **ipv6cp** | **ipx** | **ipxcp** | **lcp** | **lqc** | **mp** | **mpls-multicast packet** [**interface** *interface-type interface-number*] | **mpls-unicast packet** [**interface** *interface-type interface-number*] | **mplscp** | **osi-npdu** | **osicp** | **pap** | **scp** | **vjcomp** { **all** | **error** | **event** | **packet** | **state**} [**interface** *interface-type interface-number*] }

View User view

Default Level 1. Monitor level

Parameters **all**: All PPP debugging.

bcp: PPP Bridging Control Protocol (BCP) debugging.

cbcp: PPP Callback Control Protocol (CBCP) debugging.

ccp: PPP Compression Control Protocol (CCP) debugging.

chap: PPP CHAP debugging.

compression: PPP IP header compression (TCP and RTP) debugging.

core: PPP kernel event debugging.

ip: IP packet debugging.

ipcp: IP Control Protocol (IPCP) debugging.

ipv6: IPv6 packet debugging.

ipv6cp: IPv6 Control Protocol (IPv6CP) debugging.

ipx: IPX debugging.

ipxcp: IPX Control Protocol (IPXCP) debugging.

lcp: PPP Link Control Protocol (CCP) debugging.

lqc: PPP link quality control (LQC) debugging.

mp: MP debugging.

mpls-multicast: MPLS multicast debugging.

mpls-unicast: MPLS unicast debugging.

mplscp: MPLS Control Protocol (MPLSCP) debugging.

osi-npdu: OSI NPDU debugging.

osicp: OSI Control Protocol (OSICP) debugging.

pap: PAP debugging.

scp: Stac LZS debugging.

vjcomp: VJ TCP/IP header compression debugging.

error: PPP error debugging.

event: PPP event debugging.

packet: PPP packet debugging.

state: PPP state debugging.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **debugging ppp** command to enable PPP debugging.

Use the **undo debugging ppp** command to disable PPP debugging.

By default, all PPP debugging is disabled. The following tables describe some significant output fields of PPP debugging commands.

Table 88 Description on the fields of the debugging ppp event command

Field	Description
event	A PPP event occurred.
state	The state of a PPP state machine.
Up	The lower layer went up.
Down	The lower layer went down.
Open	The link was administratively opened.
Close	The link was administratively closed.

Table 88 Description on the fields of the debugging ppp event command

Field	Description
Timeout(T0+,T0-)	A timeout event occurred. T0+ indicates that the restart counter is greater than 0; thus, retransmission is required. T0- indicates that the restart counter is less than 0; thus, retransmission is not needed.
Receive-Configure-Request(RCR+,RCR-)	A Configure-Request packet was received from the peer. RCR+ indicates that the request is acceptable and a Configure-Ack should be sent back. RCR- indicates that the request is unacceptable, and a Configure-Nak or Configure-Rej should be sent back.
Receive-Configure-Ack(RCA)	A valid Configure-Ack packet was received from the peer. The packet is a positive response to a configuration request.
Receive-Configure-Nak/Rej(RCN)	A valid Configure-Nak/Rej packet was received from the peer. The packet is a negative response to some or all requested configuration options.
Receive-Terminate-Request(RTR)	A Terminate-Request packet was received indicating that the peer wanted to close the connection.
Receive-Terminate-Ack(RTA)	A Terminate-Ack packet was received from the peer.
Receive-Unknown-Code(RUC)	An unknown packet was received from the peer.
Receive-Code-Reject, Receive-Protocol-Reject(RXJ+,RXJ-)	A Code-Reject or Protocol-Reject packet was received from the peer. RXJ+ indicates that the rejected options are within the scope of normal operation and thus the rejection is acceptable. RXJ- indicates that the rejected options are not acceptable and link termination will result.
Receive-Echo-Request	An Echo-Request packet was received from the peer.
Receive-Echo-Reply	An Echo-Reply packet was received from the peer.
Receive-Discard-Request(RXR)	A Discard-Request packet was received from the peer.

Table 89 Description on the fields of the debugging ppp ipcp command

Field value	Field name	Description
2	*IP-Compression-Protocol*	The adopted IP compression protocol.
3	*IP Address*	IP address negotiation.
129	*Primary DNS Server Address*	Requested or allocated the primary DNS server.
130	*Primary NBNS Server Address*	Requested or allocated the primary NBNS server.

Table 89 Description on the fields of the debugging ppp ipcp command

Field value	Field name	Description
131	*Secondary DNS Server Address*	Requested or allocated a secondary DNS server.
132	*Secondary NBNS Server Address*	Requested or allocated a secondary NBNS server.

Examples # Two devices are connected using Serial interfaces. Enable PPP on the two interfaces. PPP negotiation starts between them. Enable PPP debugging.

```
*0.784906 Sysname PPP/8/debug2:
  PPP Event:
      Serial2/0 LCP Open  Event
      state initial
```

// On interface Serial 2/0, the LCP state machine was opened and was in the initial state.

```
*0.784906 Sysname PPP/8/debug2:
  PPP State Change:
      Serial2/0 LCP : initial --> starting
```

// LCP moved from the initial state to the starting state.

```
*0.784906 Sysname PPP/8/debug2:
  PPP Event:
      Serial2/0 LCP Lower Up  Event
      state starting
```

// A lower layer up event was reported for LCP. The LCP state machine was in the starting state.

```
*0.784906 Sysname PPP/8/debug2:
  PPP State Change:
      Serial2/0 LCP : starting --> reqsent
```

// LCP moved from the starting state to the reqsent state.

```
*0.784906 Sysname PPP/8/debug2:
  PPP Packet:
      Serial2/0 Output LCP(c021) Pkt, Len 35
      State reqsent, code ConfReq(01), id 2a, len 31
      MRU(1), len 4, val 05dc
      AuthProto(3), len 4, PAP c023
      MagicNumber(5), len 6, val 31180c00
      MRRU(11), len 4, val 05dc
      Discri(13), len 9, val 01fa4d432c8451
```

// Interface Serial 2/0 sent a 35-byte LCP packet. The type of the packet is Configure-Request, its ID is 2a, and its length is 31 bytes with the header removed. The LCP state machine transited to the request sent state as a result. The packet contains these configuration options for negotiation: MRU (the TLV length is four bytes, and the desired MRU value is 05dc); the authentication protocol (the TLV length is four bytes and the desired authentication protocol is PAP); the magic-number (the TLV length is 6 bytes, and the value is 31180c00); the MRRU

(the TLV length is four bytes and the desired MRRU is 05dc); and the endpoint discriminator of MP (the TLV length is 9 bytes, and the value is 01fa4d432c8451.)

36 BRIDGING CONFIGURATION COMMANDS

bridge aging-time

Syntax **bridge aging-time** *seconds*

undo bridge aging-time

View System view

Parameters *seconds*: Aging time of dynamic bridge table entries, in seconds, with an effective range of 10 to 1000000.

Description Use the **bridge aging-time** command to configure the aging time of dynamic bridge table entries.

Use the **undo bridge aging-time** command to restore the default setting.

By default, the aging time of dynamic bridge table entries is 300 seconds.

Example # Set the aging time of dynamic bridge table entries to 500 seconds.

```
<Sysname> system-view
[Sysname] bridge aging-time 500
```

bridge bridge-set enable

Syntax **bridge** *bridge-set* **enable**

undo bridge *bridge-set* **enable**

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

Description Use the **bridge** *bridge-set* **enable** command to enable a bridge set.

Use the **undo bridge** *bridge-set* **enable** command to remove a bridge set.

- *Before you can enable the bridge set feature, you need to enable bridging first.*
- *Other related configurations can take effect only if the bridging and bridge set features are enabled. This command is required for bridge configuration.*

Example # Enable bridge set 1.

```
<Sysname> system-view
[Sysname] bridge 1 enable
```

bridge bridging

Syntax **bridge** *bridge-set* **bridging** { **ip** | **ipx** | **others** }

undo bridge *bridge-set* **bridging** { **ip** | **ipx** | **others** }

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

ip: Specifies the Internet protocol (IP).

ipx: Specifies the internetwork packet exchange (IPX) protocol.

others: Specifies other protocols than IP and IPX.

Description Use the **bridge bridging** command to enable bridging of the specified network layer protocol(s) on the specified bridge set.

Use the **undo bridge bridging** command to disable bridging of the specified network layer protocol(s) on the specified bridge set.

By default, bridging of all network layer protocols is enabled.

Note that non-routable packets will be discarded if bridging of IP or IPX is disabled in a bridge set.

Example # Disable IP bridging on bridge set 1.

```
<Sysname> system-view
[Sysname] undo bridge 1 bridging ip
```

Enable IP bridging on bridge set 1.

```
<Sysname> system-view
[Sysname] bridge 1 bridging ip
```

bridge enable

Syntax **bridge enable**

undo bridge enable

View System view

Parameters None

Description Use the **bridge enable** command to enable the bridging functionality.

Use the **undo bridge enable** command to disable the bridging functionality.

By default, bridging is disabled.

Other related configurations can take effect only if the bridging and bridge set features are enabled. This command is required for bridge configuration.

Example # Enable bridging.

```
<Sysname> system-view
[Sysname] bridge enable
```

bridge learning

Syntax **bridge** *bridge-set* **learning**

undo bridge *bridge-set* **learning**

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

Description Use the **bridge learning** command to enable dynamic address learning to allow the specified bridge set to add dynamic address entries into the bridge table.

Use the **undo bridge learning** command to disable dynamic address learning.

By default, dynamic address learning is enabled, namely all bridge sets are allowed to add dynamic address entries into the bridge table.

Example # Enable dynamic address learning.

```
<Sysname> system-view
[Sysname] bridge 1 learning
```

bridge mac-address

Syntax **bridge** *bridge-set* **mac-address** *mac-address* { **deny | permit** } [**dlsw** | **interface** *interface-type interface-number*]

undo bridge *bridge-set* **mac-address** *mac-address* [**interface** *interface-type interface-number*]

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

mac-address: MAC address, in the format of H-H-H

deny: Discards frames whose source address or destination address is the specified address on all interfaces or the specified interface.

permit: Forwards frames whose source address or destination address is the specified address on all interfaces or the specified interface.

interface: Specifies an outbound interface.

interface-type interface-number: Specifies an interface by its name and number.

dlsw: Specified that the outbound interface is a DLSw module.

Description Use the **bridge mac-address** command to configure a static bridge table entry.

Use the **undo bridge mac-address** command to remove a static bridge table entry.

Example # Configure a static bridge table entry so that Ethernet1/0 can forward frames with a destination MAC address of 0000-0000-0111.

```
<Sysname> system-view
[Sysname] bridge 1 mac-address 0000-0000-0111 permit interface ethernet 1/0
```

bridge routing

Syntax **bridge** *bridge-set* **routing** { **ip** | **ipx** }

undo bridge *bridge-set* **routing** { **ip** | **ipx** }

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

ip: Specifies the Internet protocol (IP).

ipx: Specifies the internetwork packet exchange (IPX) protocol.

Description Use the **bridge routing** command to enable routing of the specified protocol(s) on the specified bridge set.

Use the **undo bridge routing** command to disable routing of the specified protocol(s) on the specified bridge set.

By default, routing of network layer protocols is disabled.

If the bridge set is configured to route the specified protocol, the packets of the protocol that need to be routed will be routed.

Example # Enable IP routing in bridge set 1.

```
<Sysname> system-view
[Sysname] bridge 1 routing ip
```

bridge routing-enable

Syntax **bridge routing-enable**

undo bridge routing-enable

View System view

Parameters None

Description Use the **bridge routing-enable** command to enable bridge routing.

Use the **undo bridge routing-enable** command to disable bridge routing.

By default, bridge routing is disabled.

Routing of a particular protocol can be implemented only if bridge routing is enabled.

Example # Enable bridge routing.

```
<Sysname> system-view
[Sysname] bridge routing-enable
```

bridge-set

Syntax **bridge-set** *bridge-set*

undo bridge-set *bridge-set*

View Interface view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

Description Use the **bridge-set** command to add the current interface into a bridge set.

Use the **undo bridge-set** command to remove the current interface from a bridge set.

By default, a bridge set does not contain any interface.

Example # Add Ethernet1/0 into bridge set 1.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] bridge-set 1
Promiscuous operation mode was set automatically.
```

- *As shown above, after being added into bridge set 1, Ethernet1/0 automatically works in the promiscuous operation mode. When working in the*

promiscuous operation mode, an Ethernet interface forwards all correct frames, without filtering any MAC address.

- *Bridging is possible only between interfaces in the same bridge set.*

As shown above, after being added into bridge set 1, Ethernet1/0 automatically works in the promiscuous operation mode. When working in the promiscuous operation mode, an Ethernet interface forwards all correct frames, without filtering any MAC address.

display bridge address-table

Syntax **display bridge address-table** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number* | **mac** *mac-address*] [**dynamic** | **static**]

View Any view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

dlsw: Displays the bridge table information about DLSw.

interface-type interface-number : Specifies an interface by its name and number.

mac-address: MAC address, in the format of H-H-H

dynamic: Displays the information about dynamically learned addresses in the bridge table.

static: Displays the information about manually configured about addresses in the bridge table.

Description Use the **display bridge address-table** command to view the bridge table information.

Example # View the information about all the manually configured entries in the bridge table.

```
<Sysname> display bridge address-table static
The total of the address-items is 1
 Mac-address     Set Flag Aging-time    Receive       Send Interface-name
 0000-0001-0001    2   NS   00:02:04          0          0  Ethernet1/0
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

View the information about a dynamically learned MAC address 1234-5678-1234 in the bridge table.

```
<Sysname> display bridge address-table mac 1234-5678-1234 dynamic
 Mac-address     Set Flag Aging-time    Receive       Send Interface-name
 1234-5678-1234    1   PD   00:02:48         36          0  Ethernet1/0
 Flag meaning:  P--PERMIT   N--DENY  D--DYNAMIC  S--STATIC
```

Table 90 Description on the fields of the display bridge address-table command

Field	Description
Mac-address	MAC address

Table 90 Description on the fields of the display bridge address-table command

Field	Description
Set	Bridge set number
Flag	Flag can be any of the four values: P--PERMIT N--DENY D--DYNAMIC S--STATIC
	P: The permit rule is used for MAC address filtering
	N: The deny rule is used for MAC address filtering
	D: This entry is a dynamic entry
	S: This entry is a static entry
Aging-time	The aging time of bridge table entries
Receive	Number of received frames destined for this MAC address
Send	Number of forwarded frames destined for this MAC address
Interface-name	Outbound interface name

display bridge information

Syntax **display bridge information** [**bridge-set** *bridge-set*]

View Any view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

Description Use the **display bridge information** command to view the information about the specified bridge set or all bridge sets.

Example # View the information about all bridge sets.

```
<Sysname> display bridge information
Bridge module is activated,2 port take part in bridge module at all;
 Address table has 15 item, with  1 static one; life cycle is 300 (s).

Bridge set 1 :
  configure :bridge 1 enable;
             bridging ip, undo bridging ipx; bridging others;
             undo routing ip, undo routing ipx;
             bridge 1 learning
  interface :total 2 interface(s) in the set
             Ethernet1/0 : up
             Ethernet1/1 : up
Bridge set 2 :
  configure :bridge 2 enable;
             bridging ip, undo bridging ipx; bridging others;
             undo routing ip, undo routing ipx;
             bridge 2 learning
  interface :total 2 interface(s) in the set
             Ethernet1/0.1 :up
             Ethernet1/0.2 :up
```

Table 91 Description on the fields of the display bridge information command

Field	Description
configure	Configuration properties of this bridge set. For example, the "configuration" part of bridge set 1 indicates that bridge set 1 can bridge IP packets, it cannot bridge IPX packets, and it can dynamically learn MAC addresses
interface	Interfaces in this bridge sets and their status, where up represents that the interface is active, while "down" represents that the interface is inactive. Bridging is possible only between active interfaces in the same bridge set.

As shown above, bridge set 1 and bridge set 2 in the system are active. The information of each bridge set includes two parts: configure and interface.

display bridge traffic

Syntax **display bridge traffic** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number*]

View Any view

Parameters *bridge-set*: Displays the statistics information about bridged traffic in the specified bridge set. *bridge-set* must be an integer in the range of 1 to 255.

dlsw: Displays the statistics information of bridged traffic that has passed the DLSw module.

interface-type interface-number: Displays the statistics information about bridged traffic that has passed the specified interface.

Description Use the **display bridge traffic** command to view the statistic information about bridged traffic.

If no parameter is provided, this command displays the statistics about all the bridged traffic on the device.

Example # View the statistics information about bridged traffic that has passed Ethernet1/0.

```
<Sysname> display bridge traffic interface ethernet 1/0
the statistic of interface Ethernet1/0 in bridge set 1 :
Input:
         10 total, 1 bpdu, 2 single,
         0 multi, 0 broadcast;
         0 ip,0 ipx, 0 other protocol;
         0 eth2, 0 snap,
         0 dlsw, 0 other,
         0 vlan;
Output:
         0 total, 0 bpdu, 0 single,
         0 multi, 0 broadcast;
         0 ip, 0 ipx, 0 other protocol;
```

```
          0 eth2, 0 snap,
          0 dlsw, 0 other,
          0 vlan;
Send way:
          0 broadcast, 0 fast, 0 other
Discard:
          0 by import state,
          0 for local frame ,
          0 by mac table,
          0 by import filter,
          0 by outport filter,
          0 by ip filter ,
          0 other
```

Table 92 Description on the fields of the display bridge traffic command

Field	Description
Input	Indicates what kinds of and how many frames were received on this interface. "10 total, 1 bpdu, 2 single," means that totally 10 frames were received on this interface, including one BPDU and two unicast packets
Output	Indicates what kinds of and how many frames were sent out on this interface
Send way	Indicates how frames were sent
Discard	Indicates why and how many frames were discarded
0 by import state	The number of frames discarded due to abnormal inbound interface state
0 for local frame	The number of frames discarded because the source address and destination address map to the same interface
0 by mac table	The number of frames discarded due to denied entries configured in the bridge table
0 by import filter	The number of frames discarded due to the filtering rules configured on the inbound interfaces
0 by outport filter	The number of frames discarded due to the filtering rules configured on the outbound interfaces
0 by ip filter	The number of frames discarded due to the filtering rules configured at the IP layer
0 other	The number of frames discarded due to other reasons

display interface bridge-template

Syntax **display interface bridge-template** [*interface-number*]

View Any view

Parameter *interface-number*: Specifies an bridge-template interface.

Description Use the **display interface bridge-template** command to display the statistics information of a bridge-template interface.

Example # Display the statistics information of bridge-template 1.

```
<Sysname> display interface bridge-template 1
Bridge-template1 current state :UP
Line protocol current state :UP
Description : Bridge-template1 Interface
The Maximum Transmit Unit is 1500
Internet Address is 2.0.0.1/30
IP Sending Frames' Format is PKTFMT_ETHNT_2, Hardware address is 000f-e207-f301
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e200-1234
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Table 93 Description on the fields of display interface bridge-template

Field	Description
Bridge-template1 current state :UP	State of the bridge-template interface
Line protocol current state	State of the data link layer protocol (UP/DOWN)
Description : : Bridge-template1 Interface	Descriptive string of the interface
The Maximum Transmit Unit	MTU of the interface
Internet Address is 2.0.0.1/30	IP address of the interface
IP Packet Frame Type	Packet encapsulation format
Hardware Address	Hardware address (MAC address)
IPv6 Packet Frame Type	IPv6 packet encapsulation formats
Output queue : (Urgent queue : Size/Length/Discards)	Statistics for output queue: ■ Packet statistics for the urgent queue ■ Packet statistics for the protocol queue ■ Packet statistics for the FIFO queue
Output queue : (Protocol queue : Size/Length/Discards)	
Output queue : (FIFO queuing : Size/Length/Discards)	
Last 300 seconds input: 0 bytes/sec 0 packets/sec Last 300 seconds output: 0 bytes/sec 0 packets/sec	Average rate at which packets are input and output through the current interface in the last 300 seconds (in bytes per second)
0 packets input, 0 bytes, 0 drops	Total number and total size in bytes of input packets and the number of dropped packets on the interface
0 packets output, 0 bytes, 0 drops	Total number and size in bytes of output packets and the number of dropped packets on the interface

fr map bridge

Syntax **fr map bridge** *dlci* **broadcast**

undo fr map bridge *dlci*

View Interface view

Parameters *dlci*: Local virtual circuit number, in the range of 16 to 1007

broadcast: Specifies to allow bridging of broadcasts over this FR-to-bridging mapping.

Description Use the **fr map bridge** command to create an FR-to-bridging mapping on the specified virtual circuit.

Use the **undo fr map bridge** command to remove an FR-to-bridging mapping.

By default, no FR-to-bridging mappings exist.

Related command: **display fr map-info** on page 376.

Example # Create an FR-to-bridging mapping on the virtual circuit by the DLCI of 50 on Serial2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] link-protocol fr
[Sysname-Serial2/0] fr interface-type dce
[Sysname-Serial2/0] fr dlci 50
[Sysname-Serial2/0] bridge-set 1
[Sysname-Serial2/0] fr map bridge 50 broadcast
```

interface bridge-template

Syntax **interface bridge-template** *bridge-set*

undo interface bridge-template *bridge-set*

View System view

Parameters *bridge-set*: Bridge set number, an integer in the range of 1 to 255.

Description Use the **interface bridge-template** command to create a bridge-template interface for a bridge set.

Use the **undo interface bridge-template** command to remove a bridge-template interface.

A bridge set can have only one bridge-template interface.

Related command: **bridge routing-enable**.

Example # Create a bridge-template interface for bridge set 1.

```
<Sysname> system-view
[Sysname] interface bridge-template 1
[Sysname-Bridge-template1]
```

mac-address (bridge-template interface view)

Syntax **mac-address** *mac-address*

undo mac-address

View Bridge-template interface view

Parameters *mac-address*: MAC address, in the format of H-H-H

Description Use the **mac-address** command to configure a MAC address for the current bridge-template interface.

Use the **undo mac-address** command to configure the configured MAC address of the current bridge-template interface.

By default, if a bridge set contains Ethernet interfaces, its bridge-template interface will use the MAC address of a random Ethernet interface. If the bridge set contains no Ethernet interfaces, its bridge-template interface will use the system default MAC address.

Related command: **interface bridge-template**.

Different models of devices may have different deferent system default MAC addresses. Refer to your specific device model.

Example # Set the MAC address of the bridge-template interface of bridge set 1 to 0000-0011-0011.

```
<Sysname> system-view
[Sysname] interface bridge-template 1
[Sysname-Bridge-template1] mac-address 0000-0011-0011
```

map bridge-group

Syntax **map bridge-group broadcast**

undo map bridge-group

View PVC view

Parameters None

Description Use the **map bridge-group broadcast** command to enable bridging over the current PVC.

Use the **undo map bridge-group** command to disable bridging over the current PVC.

By default, bridging over a PVC is disabled. If you configure both the **map bridge virtual-ethernet** and **map bridge-group** commands, only the **map bridge virtual-ethernet** takes effect.

Example # Enable bridging over PVC 32/102.

```
<Sysname> system-view
[Sysname] interface atm 1/0
[Sysname-Atm1/0] pvc 32/102
[Sysname-atm-pvc-Atm1/0-32/102] map bridge-group broadcast
```

reset bridge address-table

Syntax **reset bridge address-table** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number*]

View User view

Parameters *bridge-set*: Clears MAC address entries of the specified bridge set. *bridge-set* must be an integer in the range of 1 to 255.

dlsw: Clears MAC address entries of the DLSw module.

interface-type interface-number: Clears MAC address entry of the specified interface.

Description Use the **reset bridge address-table** command to remove one or more dynamic bridge table entries.

Example # Clear all dynamic entries about bridge set 1 from the bridge table.

```
<Sysname> reset bridge address-table bridge-set 1
```

reset bridge traffic

Syntax **reset bridge traffic** [**bridge-set** *bridge-set* | **dlsw** | **interface** *interface-type interface-number*]

View User view

Parameters *bridge-set*: Clears traffic statistics information about the specified bridge set. *bridge-set* must be an integer in the range of 1 to 255.

dlsw: Clears the traffic statistics information about the DLSw module.

interface-type interface-number: Clears the traffic statistics information about the specified interface.

Description Use the **reset bridge traffic** command to clear the statistic information about bridged traffic.

Example # Clear the traffic statistics information about bridge set 1.

```
<Sysname> reset bridge traffic bridge-set 1
```

x25 map bridge

Syntax **x25 map bridge x121-address** *x.121-address* **broadcast**

undo x25 map bridge x121-address *x.121-address*

View Interface view

Parameters **x121-address** *x.121-address*: X.121 address of the peer host.

broadcast: Enables bridging of broadcasts to the X.25 destination.

Description Use the **x25 map bridge** command to create an X.25-to-bridging mapping.

Use the **undo x25 map bridge** command to remove an X25-to-bridging mapping.

By default, no X.25-to-bridging mappings exist.

Related command: **display x25 map** on page 426.

Example # Create an X.25-to-bridging mapping on Serial2/0.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] link-protocol x25
[Sysname-Serial1/0] x25 x121-address 100
[Sysname-Serial1/0] x25 map bridge x121-address 20112451 broadcast
[Sysname-Serial1/0] bridge-set 1
```

37 ISDN CONFIGURATION COMMANDS

dialer isdn-leased (ISDN BRI interface view)

Syntax **dialer isdn-leased** { **128k** | *number* }

undo dialer isdn-leased { **128k** | *number* }

View ISDN BRI interface view

Parameter **128k**: 128 kbps ISDN leased line connection.

number: 64 kbps ISDN leased line connection. It can be 0 for the first B channel or 1 for the second B channel.

Description Use the **dialer isdn-leased 128k** command to configure 128 kbps leased line connection.

Use the **undo dialer isdn-leased 128k** command to remove 128 kbps leased line connection.

Use the **dialer isdn-leased** *number* command to configure 64 kbps leased line connection.

Use the **undo dialer isdn-leased** *number* command to remove 64 kbps leased line connection.

By default, no ISDN leased line connection is configured.

You must manually remove the existing leased line configuration before switching from single B channel leased line to 128 kbps leased line.

- *You cannot configure this command on the BRI interfaces provided by 2S1B modules.*
- *For more information about configuring ISDN leased lines on CE1/PRI and CT1/PRI interfaces, refer to "dialer isdn-leased (physical interface view)" on page 320.*

Example # Configure 128 kbps leased line connection.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] dialer isdn-leased 128k
```

display isdn active-channel

Syntax **display isdn active-channel** [**interface** *interface-type interface-number*]

View Any view

Parameter *interface-type interface-number:* Specifies an interface by its type and number.

Description Use the **display isdn active-channel** command to view the active call information on ISDN interfaces. If no interface has been specified, the system will display the active call information on all the ISDN interfaces.

The displayed information can help you with ISDN call troubleshooting.

Example # Display the active call information on the interface BRI 1/0.

```
<Sysname> display isdn active-channel interface bri 1/0
Bri 1/0
  Channel Info: B1
  Call Property: Digital        Call Type: Out
  Calling Number: -             Calling Subaddress: -
  Called Number: 6688164        Called Subaddress: -
  UserName: -                   IP Address: -
  Start Time: 05-04-30 14:27:52
  Time Used: 00:04:34
```

Table 94 Description on the fields of the display isdn active-channel command

Field	Description
Channel Info	Information about the channel
Call Property	Call property: digital or analog
Call Type	Call type: incoming or outgoing
Calling Number	Calling number
Calling Subaddress	Calling subaddress
Called Number	Called number
Called Subaddress	Called subaddress
UserName	User name used in PPP negotiation for authentication
IP Address	IP address of the peer end
Start Time	Time at which the link was set up
Time Used	Duration of the call

display isdn call-info

Syntax **display isdn call-info** [**interface** *interface-type interface-number*]

View Any view

Parameter *interface-type interface*-number: Specifies an interface by its type and number.

Description Use the **display isdn call-info** command to view the current state of ISDN interfaces. If no interface has been specified, the system will display the current states of all the ISDN interfaces.

Executing this command will output the state of each layer of the ISDN protocol on one or all interfaces, including the information of Q.921, Q.931 and CC modules. You may make troubleshooting based on the output information.

Example # Display the current state of ISDN interface 2/0.

```
<Sysname> display isdn call-info interface bri 2/0
Bri 2/0(User-side): ACTIVE
  Link Layer 1:  TEI = 65, State = MULTIPLE_FRAME_ESTABLISHED
  Link Layer 2:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 3:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 4:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 5:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 6:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 7:  TEI = NONE, State = TEI_UNASSIGNED
  Link Layer 8:  TEI = NONE, State = TEI_UNASSIGNED
  Network Layer: 1 connection(s)
    Connection 1 :
      CCIndex:0x0055 , State: Active , CES:1 , Channel:0x00000001
      TEI: 65
      Calling_Num[:Sub]:
      Called_Num[:Sub]: 6688164
```

Table 95 Description on the fields of the display isdn call-info command

Field	Description
BRI 2/0(User-side): ACTIVE	Interface BRI 2/0 is operating at the user side of ISDN; the D channel is active
Link Layer 1	Connections 1 through 8 at layer 2 of the BRI interface
…	
Link Layer 8	
TEI	Terminal equipment identifier
State	Current state of the layer 2 link. It can be one of the following:
	TEI_UNASSIGNED
	ASSIGN_AWAITING_TEI
	ESTABLISH_AWAITING_TEI
	TEI_ASSIGNED
	AWAITING_ESTABLISHMENT
	AWAITING_RELEASE
	MULTIPLE_FRAME_ESTABLISHED
	TIMER_RECOVER
	TEI_ASSIGNED_EXT1: a state option for TBR3 test, meaning a deactivation instruction is received from the underlying layer
	TEI_ASSIGNED_EXT2: a state option for TBR3 test, meaning link establishment request is received
Network Layer: 1 connection(s)	Only one network layer connection is present on the interface.

Table 95 Description on the fields of the display isdn call-info command

Field	Description
CCIndex	Index of the call at the CC layer
State	Current state of the layer 3 link of the BRI interface. It can be one of the following:
	NULL
	CALL_INITIATED
	OVERLAP_SENDING
	OUTGOING_CALL_PROCEEDING
	CALL_DELIVERED
	CALL_PRESENT
	CALL_RECEIVED
	CONNECT_REQUEST
	INCOMING_CALL_PROCEEDING
	ACTIVE
	DISCONNECT_REQUEST
	DISCONNECT_INDICATION
	SUSPEND_REQUEST
	RESUME_REQUEST
	RELEASE_REQUEST
	OVERLAP_RECEIVING
CES	Connection endpoint suffix
Channel	ISDN B channel map for the call
Calling_Num[:Sub]:	Calling number: calling sub-address.
Called_Num[:Sub]	Called number: called sub-address

display isdn call-record

Syntax **display isdn call-record** [**interface** *interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display isdn call-record** command to view the information of ISDN call history. If no interface is specified, the system displays all ISDN call history.

Executing this command will display information of the calls activated up to now, but the number of retained entries is limited to 100.

Example # Display the information of ISDN call history.

```
<Sysname> display isdn call-record
Call Calling     Called    Start               Stop           Seconds
Type Number      Number    Time                Time              Used
In   10660016  10660016    03-07-05 11:23:09   -                  0
In   10660022  10660022    03-07-05 11:23:09   -                  0
```

```
Out   -          660016       03-07-05 11:23:01   03-07-05 11:23:04  3
Out   -          660022       03-07-05 11:23:01   03-07-05 11:23:04  3
In    10660016   10660016     03-07-05 11:23:01   03-07-05 11:23:04  3
In    10660022   10660022     03-07-05 11:23:01   03-07-05 11:23:04  3
```

Table 96 Description on the fields of the display isdn call-record command

Field	Description
Call Type	Call type: incoming or outgoing
Calling Number	Calling number
Called Number	Called number
Start Time	Time at which the call is set up
Stop Time	Time at which the call is terminated
Seconds Used	Duration of the call in seconds

display isdn parameters

Syntax **display isdn parameters** { *protocol* | **interface** *interface-type interface-number* }

View Any view

Parameter *protocol*: ISDN protocol type, which can be **ans**, **at&t**, **dss1**, **etsi**, **ni**, **ni2**, **ntt**, or **qsig**.

interface-type interface-number*:* Specifies an interface by its type and number.

Description Use the **display isdn parameters** command to view the system parameters at layers 2 and 3 of the ISDN protocol, such as the durations of system timers and frame size.

If only ISDN protocol is specified, the system will display the default system parameters of ISDN.

Example # Display the system parameters of the ISDN protocol DSS1.

```
<Sysname> display isdn parameters dss1
DSS1 ISDN layer 2 system parameters:
 T200(sec)   T201(sec)   T202(sec)    T203(sec)   N200   K(Bri)    K(Pri)
  1           1           2            10          3      1         7

DSS1 ISDN layer 3 system timers:
  Timer-Number      Value(sec)
  T301                    240
  T302                    15
  T303                    4
  T304                    30
  T305                    30
  T308                    4
  T309                    90
  T310                    40
  T313                    4
  T314                    4
  T316                    120
  T317                    10
  T318                    4
  T319                    4
```

```
T321                    30
T322                    4
```

Table 97 Description of the fields of the display isdn parameters command

Item	Description
T200(sec)	Retransmit-timer (in seconds) of the L2 protocol of ISDN
T201(sec)	TEI test request retransmit-timer (in seconds) of the L2 protocol of ISDN
T202(sec)	TEI request retransmit-timer (in seconds) of the ISDN L2 protocol
T203(sec)	The maximum link idle time (in seconds) of the ISDN L2 protocol
N200	The maximum number of retransmissions
K(BRI)	The maximum number of unacknowledged frames (slide window size) on the ISDN BRI port
K(PRI)	The maximum number of unacknowledged frames (slide window size) on the ISDN PRI port
Timer-Number	ISDN L3 timer
Value(sec)	Duration (in seconds) of each ISDN L3 timer

display isdn spid

Syntax **display isdn spid** [**interface** *interface-type interface-number*]

View Any view

Parameter *interface-type interface-number:* Specifies an interface by its type and number.

Description Use the **display isdn spid** command to view information on SPID on the BRI interface encapsulated with the NI protocol.

You may execute this command to view the SPID type, SPID value and some other information when ISDN is running. Executing this command without specifying an interface, you may view information on SPI on all the SPID-supported BRI interfaces.

Example # Display the related information of SPID on the NI-supported interface BRI 1/0.

```
<Sysname> display isdn spid interface bri 1/0
Interface Bri1/0 :
  SPID Type: AUTO

  SPID B1:
  SPID Num:
  Neg State: SPID_UNASSIGNED
  Init State: INIT_NULL

  SPID B2:
  SPID Num:
  Neg State: SPID_UNASSIGNED
  Init State: INIT_NULL
```

```
SPID timer: 30 seconds
SPID resend: 1 times
```

Table 98 Description on the fields of the display isdn spid interface command

Field	Description
SPID Type	SPID Type, which can be NIT, STATIC (having only the L3 initialization process), or AUTO (including both the negotiation and the L3 initialization)
SPID B1	SPID value of the BRI interface B1 channel.
SPID Num	SPID value of the BRI interface. It can be a static configuration or the result of a dynamic negotiation, all depending on the specified SPID Type.
Neg State	Negotiation state of the SPID, which can be SPID_UNASSIGNED, ASSIGN_AWAITING_SPID, SPID_ASSIGNED, ASSIGN_AWAITING_CALL_CLEAR.
Init State	Initialization state of the SPID, which can be INIT_NULL, INIT_IND, INIT_PROCEEDING, INIT_END, INIT_AWAITING_CALL_CLEAR.
SPID B2	SPID value of the BRI interface B2 channel.
SPID timer	Duration of the timer TSPID
SPID resend	SPID message retransmission times

isdn bch-local-manage

Syntax **isdn bch-local-manage** [**exclusive**]

undo isdn bch-local-manage

View ISDN interface view

Parameter **exclusive**: Exclusive local management mode for ISDN B channels. When the B channel indicated by the exchange is inconsistent with the one required by the local end, call failure occurs.

Description Use the **isdn bch-local-manage** command to enable local ISDN B channel management.

Use the **undo isdn bch-local-manage** command to disable the setting.

By default, the local ISDN B channel management is not enabled but is in the charge of ISDN switch.

It is very important to put appropriate control on the B channels used for calls in process, especially in the PRI mode. Proper channel management can improve call efficiency and reduce call loss. Normally, the centralized B channel management provided by exchanges can work well. For this reason, you are recommended to adopt the management function provided by exchanges in most cases, despite the ISDN module can provide the channel management function as well.

Configured with **isdn bch-local-manage** command, the router operates in local B-channel management mode to select available B channels for calls. Despite this, the connected exchange has higher priority in B channel selection. If the B channel

the router selected for a call is different from the one indicated by the exchange, the one indicated by the exchange is used for communication.

Configured with the **isdn bch-local-manage exclusive** command, the router operates in exclusive local B-channel management mode. In this mode, the B channel selected by the router must be adopted for communication. In the Channel ID information element of the call Setup message sent for a call, the router indicates that the B channel is mandatory and unchangeable. If the connected exchange indicates a B channel different from the one selected by the router, call failure occurs.

Example # Enable interface BRI 2/0 local ISDN B channel management.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn bch-local-manage
```

isdn bch-select-way

Syntax **isdn bch-select-way** { **ascending** | **descending** }

View ISDN interface view

Parameter **ascending**: Selects B channels in ascending order.

descending: Selects B channels in descending order.

Description Use the **isdn bch-select-way** command to set a B channel selection method but it does not work when the switch manages ISDN B channel. Meanwhile, the setting of **isdn bch-select-way** is a waste without configuring **isdn bch-local-manage** command on the user side.

When operating in B channel local management mode, the router selects B channels in ascending order by default.

Example # Configure B channel selection method on the interface BRI 2/0 to descending order.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn bch-select-way descending
```

isdn caller-number

Syntax **isdn caller-number** *caller-number*

undo isdn caller-number

View ISDN interface view

Parameter *caller-number*: Caller number that an incoming ISDN call can carry, which is a character string of 1 to 24 characters.

Description Use the **isdn caller-number** command to configure the range of the numbers that the router can receive.

Use the **undo isdn caller-number** command to delete the configured caller number.

Example # Configure the router to receive only the incoming calls from the caller numbers with 400.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0]isdn caller-number 400
```

isdn calling

Syntax **isdn calling** *calling-number*

undo isdn calling

View ISDN interface view

Parameter *calling-number*: Calling number.

Description Use the **isdn calling** command to have the messages from a calling party to a called party carry the calling number. This command mainly applies on BRI interfaces. If a calling party has configured this command on its BRI interface, the call party will be able to see the calling number by viewing the call history information.

Use the **undo isdn calling** command to delete calling number in the messages that a calling party transmitted.

Example # Configure the message from a calling party to a called party on interface BRI 1/0 to carry calling number.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn calling 8060170
```

isdn check-called-number

Syntax **isdn check-called-number** *check-index called-party-number* [: *subaddress*]

undo isdn check-called-number *check-index*

View ISDN interface view.

Parameter *check-index*: Called number or subaddress checking index, which is in the range of 1 to 3.

called-party-number: Called number, a string of 1 to 20 digits.

subaddress: Subaddress, which is a string of digits and/or case-insensitive English letters and is 1 to 20 characters in length.

Description Use the **isdn check-called-number** command to configure the called number or subaddress that the system should verify when receiving a digital call.

Use the **undo isdn check-called-number** command to remove the configuration.

By default, the system does not check the called number or subaddress carried by incoming digital calls.

This command is used for setting the examined item when a digital call is received. If a subaddress is specified, the system will deny an incoming digital call if the calling party sends a wrong subaddress or does not send at all.

Example # Check whether the called number carried by incoming digital calls is 66668888 on the interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn check-called-number 1 66668888
```

isdn check-time

Syntax **isdn check-time** *date-time*

undo isdn check-time

View System view

Parameter *date-time*: Time to be set when ISDN call checking is launched, in the format of **HH:MM**.

Description Use the **isdn check-time** command to enable ISDN call checking and set the time when ISDN call checking is launched.

Use the **undo isdn check-time** command to restore the default.

By default, ISDN call checking is disabled.

With ISDN call checking enabled, the system checks to see whether or not the call control blocks of the CC module and the Q.931 module are synchronized by checking all the ISDN call records on the set time point every day. The ISDN calls whose call control blocks are not synchronized are released.

Example # Enable ISDN call checking and set the time to launch ISDN call checking to 08:30.

```
<Sysname> system-view
[Sysname] isdn check-time 8:30
```

isdn crlength

Syntax **isdn crlength** *call-reference-length*

undo isdn crlength

View ISDN interface view

Parameter *call-reference-length*: ISDN call reference length, which can be one or two bytes.

Description Use the **isdn crlength** command to set length of the call reference used when a call is placed on an ISDN interface.

Use the **undo isdn crlength** command to restore the default ISDN call reference length on the interface.

By default, the call reference length is two bytes for E1 PRI and T1 PRI interfaces and one byte for BRI interfaces.

Call reference is equal to the sequence number that the protocol assigns to each call. It is one or two bytes in length and can be used cyclically.

When the router receives a call from a remote device, it can automatically identify the length of the call reference. However, some devices on the network do not have such capability. In the event that the router is required to place calls to such a device connected to it, you must configure the router to use the same call reference length configured on the connected device.

*You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.*

Example # Set the call reference length carried by the ISDN messages on the PRI interface serial/0:15 to 1 byte.

```
<Sysname> system-view
[Sysname] interface serial1/0:15
[Sysname-Serial1/0:15] isdn crlength 1
```

isdn ignore connect-ack

Syntax **isdn ignore connect-ack**

undo isdn ignore connect-ack

View ISDN interface view

Parameter None

Description Use the **isdn ignore connect-ack** command to configure the router to switch the ISDN protocol state to ACTIVE to start the data and voice service communications after sending a CONNECT message without having to wait for a CONNECT ACK message. Use the **undo isdn ignore connect-ack** command to restore the default setting.

By default, in the event that the router is communicating with an exchange, the ISDN protocol must wait for the CONNECT ACK message in response to the CONNECT message before it can switch to the ACTIVE state to start data and voice service communications.

- *In the event that the router is communicating with an ISDN exchange, its settings must be the same as those on the exchange.*
- *You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.*

Example # Set the call process on the BRI interface 1/0 to proceed to the ACTIVE state without waiting for CONNECT ACK messages.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn ignore connect-ack
```

isdn ignore hlc

Syntax **isdn ignore hlc**

undo isdn ignore hlc

View ISDN interface view

Parameter None

Description Use the **isdn ignore hlc** command to disable ISDN to carry the higher layer compatibility (HLC) information element in the SETUP messages sent when placing voice calls.

Use the **undo isdn ignore hlc** command to configure ISDN to carry the HLC information element in SETUP messages.

By default, HLC information element is carried in SETUP messages when placing voice calls.

- *In the event that the router is communicating with an ISDN exchange, its settings must be the same as those on the exchange.*
- *You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.*

Example # Configure ISDN to carry the HLC information element in the SETUP messages for the voice calls placed on the BRI interface 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn ignore hlc
```

isdn ignore llc

Syntax **isdn ignore llc**

undo isdn ignore llc

View ISDN interface view

Parameter None

Description Use the **isdn ignore llc** command to disable ISDN to carry the Lower Layer Compatibility (LLC) information element in the SETUP messages sent when placing voice calls.

Use the **undo isdn ignore llc** command to configure ISDN to carry the LLC information element in SETUP messages.

By default, LLC information element is carried in SETUP messages when placing voice calls.

- *In the event that the router is communicating with an ISDN exchange, its settings must be the same as those on the exchange.*
- *You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.*

Example # Disable ISDN to carry the LLC information element in the SETUP messages for the voice calls placed on the interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn ignore llc
```

isdn ignore sending-complete

Syntax **isdn ignore sending-complete** [**incoming** | **outgoing**]

undo isdn ignore sending-complete [**incoming** | **outgoing**]

View ISDN interface view

Parameter **incoming**: Ignores the Sending Complete Information Element in Setup messages when receiving a call.

outgoing: Sends Setup messages without the Sending Complete Information Element when placing a call.

Description Use the **isdn ignore sending-complete** command to configure the ISDN protocol to ignore the Sending Complete Information Element in Setup messages when receiving a call, or to send Setup messages without the Sending Complete Information Element when placing a call.

Use the **undo isdn ignore sending-complete** command to restore the default setting.

As for the data exchange performed between a router and an ISDN switch, the default is as follows.

- For an incoming call, the router checks the received Setup messages for the Sending Complete Information Element to determine whether or not the number is received completely. If a Setup message does contain the Sending Complete Information Element, the number is not received completely.
- For outgoing calls, a Setup message containing the Sending Complete Information Element indicates that the number is sent completely.

If you execute the **isdn ignore sending-complete** command with no keyword specified, the Sending Complete Information Element-related operations are performed when a router receives a call or places a call.

- *In the event that the router is communicating with an ISDN exchange, its settings must be the same as those on the exchange.*
- *Only with DSS1, QSIG or ETSI on interface ISDN protocol can this command be configured.*

You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by

executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.

You can configure this command on an interface only when the ISDN protocol running on the interface is DSS1, Q.SIG, NI2, or ETSI.

Example # Ignore the Sending Complete Information Element in the received SETUP messages.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn ignore sending-complete incoming
```

Disable carrying the Sending Complete Information Element in the transmitted SETUP messages.

```
[Sysname-Bri1/0] isdn ignore sending-complete outgoing
```

isdn L3-timer

Syntax **isdn L3-timer** *timer-name time-interval*

undo isdn L3-timer { **all** | *timer-name* }

View ISDN interface view

Parameter *timer-name*: Name of a L3 timer of the ISDN protocol.

time-interval: Timer duration, which can take on one of the values listed in the following table.

all: Restores the default durations of all the L3 timers.

Table 99 Description of Q931 timers

timer-name	Timer-name	Value range (in seconds)	Default (in seconds)
t301	T301	30 to 1200	240
t302	T302	5 to 60	15
t303	T303	2 to 10	4
t304	T304	10 to 60	30
t305	T305	4 to 30	30
t308	T308	2 to 10	4
t309	T309	10 to 180	90
t310	T310	10 to 180	40
t313	T313	2 to 10	4
t316	T316	20 to 180	120
t322	T322	2 to 10	4

Description Use the **isdn L3-timer** command to configure the duration of an ISDN protocol L3 timer. Use the **undo isdn L3-timer** command to restore the default duration of the ISDN L3 timer on the interface.

You can view the default durations of the L3 timers in the ISDN protocol by executing the **display isdn parameters** command.

Example # Set the duration of the L3 timer T301 on the interface BRI 1/0 to 160 seconds.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn l3-timer t301 160
```

isdn link-mode

Syntax **isdn link-mode p2p**

undo isdn link-mode

View ISDN BRI interface

Parameter None

Description Use the **isdn link-mode p2p** command to configure a BRI interface to operate in the point-to-point mode.

Use the **undo isdn link-mode** command to restore the default BRI interface operating mode.

By default, a BRI interface operates in the point-to-multipoint mode, in which a BRI interface operating on the network side can have multiple end devices attached to it.

Example # Configure BRI1/0 interface to operate in the point-to-point mode.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn link-mode p2p
```

isdn number-property

Syntax **isdn number-property** *number-property* [**calling** | **called**] [**in** | **out**]

undo isdn number-property [**calling** | **called**] [**in** | **out**]

View ISDN interface view

Parameter *number-property*: Type and number scheme of ISDN numbers. The argument takes on a hex value in the range of 0 to 7F. When it is expressed in 8 bits, bits 1 through 4 represent the code scheme, bits 5 through 7 represent the code type, and bit 8 is

reserved. The following table lists the possible number types and code schemes. For more information, see the related protocol reference manual.

Table 100 Types and code schemes of ISDN numbers

Protocol	Field (Bit) value								Definition
		Type			Code scheme				
	8	7	6	5	4	3	2	1	
		Type			Code scheme				
	8	7	6	5	4	3	2	1	
ANSI		0	0	0					User-specified
		0	1	0					National network identification
		0	1	1					International network identification
					0	0	0	0	Unknown/user-specified
					0	0	0	1	Carrier identification code
					0	0	1	1	Data network identification code (ITU-T Recommendation X.121)
AT&T		0	0	0					Unknown
		0	0	1					International number
		0	1	0					National number
		1	0	0					Subscriber number
					0	0	0	0	Unknown
					0	0	0	1	ISDN/telephony numbering loan (Recommendation E.164/E.163)
					1	0	0	1	Private numbering plan
DSS1		0	0	0					Unknown
		0	0	1					International number
		0	1	0					National number
		0	1	1					Network specific number
		1	0	0					Subscriber number
		1	1	0					Abbreviated number
		1	1	1					Reserved for extension
					0	0	0	0	Unknown
					0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
					0	0	1	1	Data numbering plan (Recommendation X.121)
					0	1	0	0	Telex numbering plan (Recommendation F.69)
					1	0	0	0	National standard numbering plan
					1	0	0	1	Private numbering plan
					1	1	1	1	Reserved for extension
ETSI		0	0	0					Unknown
		0	0	1					International number
		0	1	0					National number
		0	1	1					Network specific number
		1	0	0					Subscriber number

Table 100 Types and code schemes of ISDN numbers

Protocol	Field (Bit) value								Definition
		Type			Code scheme				
	8	7	6	5	4	3	2	1	
		1	1	0					Abbreviated number
		1	1	1					Reserved for extension
					0	0	0	0	Unknown
					0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
					0	0	1	1	Data numbering plan (Recommendation X.121)
					0	1	0	0	Telex numbering plan (Recommendation F.69)
					1	0	0	0	National standard numbering plan
					1	0	0	1	Private numbering plan
					1	1	1	1	Reserved for extension
NI		0	0	0	0	0	0	0	Unknown number in Unknown numbering plan
		0	0	1	0	0	0	1	International number in ISDN numbering plan (Rec. E.164)
		0	1	0	0	0	0	1	National number in ISDN numbering plan (Rec. E.164)
		0	1	1	1	0	0	1	Network specific number in private numbering plan
		1	0	0	0	0	0	1	Local (directory) number in ISDN numbering plan (Rec. E.164)
		1	1	0	1	0	0	1	Abbreviated number in private numbering plan
NTT		0	0	0					Unknown
		0	1	0					National number
		0	1	1					Network specific number
		1	0	0					Subscriber number
					0	0	0	0	Unknown
					0	0	0	1	ISDN/telephony numbering plan (Recommendation E.164)
					1	0	0	1	Private numbering plan
QSIG		0	0	0	0	0	0	0	Unknown number in Unknown numbering plan
		0	0	0	0	0	0	1	Unknown number in ISDN/Telephony numbering plan (ITU-T Rec.E.164/E.163)
		0	0	1	0	0	0	1	International number in ISDN/Telephony numbering plan (ITU-T Rec.E.164/E.163)
		0	1	0	0	0	0	1	National number in ISDN/Telephony numbering plan (ITU-T Rec.E.164/E.163)
		0	1	1	0	0	0	1	Subscriber number in ISDN/Telephony numbering plan (ITU-T Rec.E.164/E.163)
		0	0	0	1	0	0	1	Unknown number in private numbering plan

Table 100 Types and code schemes of ISDN numbers

Protocol	Field (Bit) value								Definition
		Type			Code scheme				
	8	7	6	5	4	3	2	1	
		0	0	1	1	0	0	1	Level 2 regional number in private numbering plan
		0	1	0	1	0	0	1	Level 1 regional number in private numbering plan
		0	1	1	1	0	0	1	PISN specific number in private numbering plan
		1	0	0	1	0	0	1	Level 0 regional number in private numbering plan

The undefined bits in all the protocols are reserved for other purposes.

calling: The specified number property is for calling numbers.

called: The specified number property is for called numbers.

in: The specified number property is for calling numbers and called numbers in incoming ISDN calls.

out: The specified number property is for calling numbers and called numbers in outgoing ISDN calls.

Description

Use the **isdn number-property** command to set the type and code scheme of calling or called numbers in incoming or outgoing ISDN calls.

Use the **undo isdn number-property** command to restore the default.

By default, the system selects ISDN number type and code scheme depending on upper layer service.

If the **isdn number-property** command is configured, the system adopts the configured ISDN number type and code scheme without considering the upper layer service.

The following table shows how to set number type and code scheme.

Table 101 Set the type and code scheme of ISDN numbers

Operation	Command
Set a number type and code scheme for the called numbers in incoming calls	**isdn number-property** *number-property* **called in**
Remove the number type and code scheme for the called numbers in incoming calls	**undo isdn number-property called in**
Set a number type and code scheme for the called numbers in outgoing calls	**isdn number-property** *number-property* **called out**
Remove the number type and code scheme for the called numbers in outgoing calls	**undo isdn number-property called out**
Set a number type and code scheme for the calling numbers in incoming calls	**isdn number-property** *number-property* **calling in**

Table 101 Set the type and code scheme of ISDN numbers

Operation	Command
Remove the number type and code scheme for the calling numbers in incoming calls	**undo isdn number-property calling in**
Set a number type and code scheme for the calling numbers in outgoing calls	**isdn number-property** *number-property* **calling out**
Remove the number type and code scheme for the calling numbers in outgoing calls	**undo isdn number-property calling out**
Set a number type and code scheme for the calling numbers in incoming and outgoing calls	**isdn number-property** *number-property* **calling**
Remove the number type and code scheme for the calling numbers in incoming and outgoing calls	**undo isdn number-property calling**
Set a number type and code scheme for the called numbers in incoming and outgoing calls	**isdn number-property** *number-property* **called**
Remove the number type and code scheme for the called numbers in incoming and outgoing calls	**undo isdn number-property called**
Set a number type and code scheme for the calling and called numbers in incoming calls	**isdn number-property** *number-property* **in**
Remove the number type and code scheme for the calling and called numbers in incoming calls	**undo isdn number-property in**
Set a number type and code scheme for the calling and called numbers in outgoing calls	**isdn number-property** *number-property* **out**
Remove the number type and code scheme for the calling and called numbers in outgoing calls	**Undo isdn number-property out**
Set a number type and code scheme for the calling and called numbers in incoming and outgoing calls	**isdn number-property** *number-property*
Remove the number type and code scheme for the calling and called numbers in incoming and outgoing calls	**undo isdn number-property**

Example # On interface BRI 1/0, set both number type and code scheme of calling numbers in incoming ISDN calls to unknown.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn number-property 0 calling in
```

On interface BRI 1/0, set both number type and code scheme of called numbers in outgoing ISDN calls to unknown.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn number-property 0 called out
```

isdn overlap-sending

Syntax **isdn overlap-sending** [*digits*]

undo isdn overlap-sending

View ISDN interface view

Parameter *digits*: Maximum number of digits that can be sent each time in overlap-sending mode, in the range 1 to 15. The default is 10.

Description Use the **isdn overlap-sending** command to set the system to send the called number information in the overlap mode on the ISDN interface.

Use the **undo isdn overlap-sending** command to set the system to send the called information in full mode.

In overlap-sending mode, the digits of each called number will be sent separately and the number of the digits sent each time can be set using this command.

In full-sending mode, all the digits of each called number will be collected and sent at a time.

By default, full-sending mode applies.

You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.

Overlap-sending is only suitable for five ISDN protocols: ANSI, DSS1, ETSI, NI, and QSIG.

Example # Apply the overlap-sending function on the interface BRI 1/0 and set the number of digits allowed to send each time to 12 digits.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn overlap-sending 12
```

isdn pri-slipwnd-size

Syntax **isdn pri-slipwnd-size** *window-size*

isdn pri-slipwnd-size default

View Interface view

Parameter *window-size*: Slide window size in the range of 5 to 14. By default, the slide window size on PRI interfaces is 7.

Description Use the **isdn pri-slipwnd-size** command to set the slide window size on a PRI interface.

Use the **isdn pri-slipwnd-size default** command to restore the default slide window size on the PRI interface.

Example # Configure the slide window size on the interface CE1/PRI 1/0 to 10.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-E1 1/0] using ce1
[Sysname-E1 1/0] quit
[Sysname]interface serial 1/0:15
[Sysname-Serial1/0:15] isdn pri-slipwnd-size 10
```

isdn protocol-mode

Syntax **isdn protocol-mode { network | user }**

undo isdn protocol-mode

View Interface view

Parameter *mode*: ISDN protocol mode to be set, which can be **network** (for network side mode) and **user** (for user side mode).

Description Use the **isdn protocol-mode** command to set the protocol mode for an ISDN interface.

Use the **undo isdn protocol-mode** command to restore the default protocol mode.

By default, an ISDN interface operates in the user side mode.

Example # Set the protocol mode to network side mode for BRI 2/0 interface (assuming that the interface is a BSV interface).

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn protocol-mode network
```

isdn protocol-type

Syntax **isdn protocol-type** *protocol*

undo isdn protocol-type

View ISDN interface view

Parameter *protocol*: ISDN protocol, which can be **ANSI**,**AT&T**, **DSS1**, **ETSI**, **NI**, **NI2**,**NTT**, or **QSIG**.

Description Use the **isdn protocol-type** command to set the ISDN protocol to be run on an ISDN interface.

Use the **undo isdn protocol-type** command to restore the default.

By default, both BRI and PRI interfaces run ISDN protocol DSS1.

You are allowed to configure:

- ANSI ISDN on BRI and T1 PRI interfaces;
- AT&T ISDN on T1 PRI interfaces;
- DSS1 ISDN on BRI, E1 PRI, and T1 PRI interfaces;
- ETSI ISDN on BRI, E1 PRI, and T1 PRI interfaces;
- NI (National ISDN) on BRI interfaces;
- NI2 (National ISDN) on T1 PRI interfaces;
- QSIG ISDN on E1 PRI and T1 PRI interfaces;
- NTT ISDN on BRI and T1 PRI interfaces.

You are not allowed to configure this command on an ISDN interface if there is still a call on it. This command can take effect only if it is configured when there is no call on the interface. Alternatively, you can manually disable the interface by executing the **shutdown** command, configure the command, and then enable the interface by executing the **undo shutdown** command. The operations, however, will lead to the disconnection of the call existing on the interface.

Example # Apply ISDN ETSI on interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn protocol-type etsi
```

isdn q921-permanent

Syntax **isdn q921-permanent**

undo isdn q921-permanent

View ISDN BRI interface view

Parameter None

Description Use the **isdn q921-permanent** command to enable the Q.921 permanent link function.

Use the **undo isdn q921-permanent** command to disable the Q.921 permanent link function.

After you enable the function, the ISDN BRI interface automatically sets up and maintains one or two Layer 2 links, whether Layer 3 calls are present on it or not. Two Layer 2 links involves when two-TEI mode is enabled on the interface.

Example # Enable the Q.921 permanent link function on interface BRI 2/0.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn q921-permanent
```

isdn send-restart

Syntax **isdn send-restart**

undo isdn send-restart

View System view

Parameter None

Description Use the **isdn send-restart** command to enable PRI interfaces to actively send ISDN RESTART messages.

Use the **undo isdn send-restart** command to disable PRI interfaces to actively send ISDN RESTART messages.

After the function is enabled, PRI interfaces actively send RESTART messages. to clear calls of the remote end before maintaining B channels.

By default, the PRI interface actively sends RESTART messages to the remote end before maintaining B channels.

Example # Enable the PRI interface to send RESTART messages before maintaining B channels.

```
<Sysname> system-view
[Sysname] isdn send-restart
```

isdn spid auto_trigger

Syntax **isdn spid auto_trigger**

View ISDN BRI interface view

Parameter None

Description Use the **isdn spid auto_trigger** command to enable SPID auto-negotiation once on the BRI interface running the NI protocol.

On a BRI interface compliant with the North American ISDN protocol, the router can place a call only after SPID negotiation or initialization. SPID information can be obtained via static configuration or dynamic negotiation. You may manually trigger a new SPID negotiation request by executing this command if the SPID negotiation in dynamic negotiation fails or just for the purpose of testing.

By default, a BRI interface does not originate a SPID negotiation request unless triggered by a call.

This command applies only on the BRI interface running the NI protocol.

Example # Manually trigger a new SPID negotiation request on the interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid auto_trigger
```

isdn spid nit

Syntax **isdn spid nit**

undo isdn spid nit

View ISDN BRI interface view

Parameter None

Description Use the **isdn spid nit** command to set the SPID processing mode to NIT (Not Initial Terminal) on an NI-compliant BRI interface.

Use the **undo isdn spid nit** command to disable the NIT mode on the BRI interface.

By default, NIT mode does not apply on BRI interfaces. Instead, static SPID or dynamic SPID negotiation is applied.

On an NI-compliant BRI interface, calls can be placed only after the SPID negotiation or initialization is finished. When the router is communicating with an NI-compliant exchange that does not support SPID negotiation, you can use this command to set the SPID processing mode on the router to NIT and the ISDN will ignore ISPID negotiation and initialization.

This command applies only on NI-compliant BRI interfaces.

Example # Ignore SPID negotiation and initialization on the interface BRI 1/0, adopting the NIT mode.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid nit
```

isdn spid timer

Syntax **isdn spid timer** *seconds*

undo isdn spid timer

View ISDN BRI interface view

Parameter *seconds*: Duration of the SPID timer, which is in the range of 1 to 255 seconds, and defaults to 30 seconds.

Description Use the **isdn spid timer** command to set the duration of the timer TSPID for an NI-compliant BRI interface to *seconds*.

Use the **undo isdn spid timer** command to restore the default duration of the timer TSPID for the NI-compliant BRI interface.

On a BRI NI-compliant interface, calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. The timer TSPID is started when the terminal originates a negotiation or initialization request by sending the INFORMATION message. You can use this command to modify the duration of TSPID.

This command applies only on NI-compliant BRI interfaces.

Example # Set the duration of TSPID on the interface BRI 1/0 to 50 seconds.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid timer 50
```

isdn spid service

Syntax **isdn spid service** [**audio** | **data** | **speech**]

undo isdn spid service

View ISDN BRI interface view

Parameter **audio**: Supports audio service.

data: Supports data service.

speech: Supports voice service.

Description Use the **isdn spid service** command to configure the service types that must be supported in SPID negotiation on the BRI interface adopting NI protocol.

Use the **undo isdn spid service** command to delete the service types that must be supported in SPID negotiation on the BRI interface adopting NI protocol.

There are three types of services. You can select any one or none. None means all services are supported. By default, SPID needs to support data and voice service simultaneously.

Generally, as for the BRI interface adopting the ISDN NI protocol, you need to negotiate or initialize SPID before originate a call. During negotiation, SPCS may send multiple SPIDs and carry the service types supported by the SPID, therefore, the router needs to choose a proper SPID according to the local service type.

This command can only be applied on the BRI interface adopting NI protocol.

Example # Set the service type supported by BRI interface to data and voice.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid service data
[Sysname-Bri1/0] isdn spid service speech
```

isdn spid resend

Syntax **isdn spid resend** *times*

undo isdn spid resend

View ISDN BRI interface view

Parameter *times*: The number of INFORMATION message retransmission attempts with an integer in the range of 1 to 255 times, which defaults to 1.

Description Use the **isdn spid resend** command to set the number of INFORMATION message retransmission attempts for SPID negotiation or initialization on an NI-compliant BRI interface.

Use the **undo isdn spid resend** command to restore the default number of INFORMATION message retransmission attempts on the interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. The timer TSPID is started when the terminal originates a negotiation or initialization request by sending the INFORMATION message. If the terminal does not receive any response upon the expiration of TSPID, it will retransmit the INFORMAITON message. You can use this command to modify the number of INFORMATION message retransmission attempts.

This command applies only on NI-compliant BRI interfaces.

Example # Set the allowed number of INFORMATION retransmission attempts to five.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid resend 5
```

isdn spid1

Syntax **isdn spid1** *spid* [*LDN*]

undo isdn spid1

View ISDN BRI interface view

Parameter *spid*: String of 1 to 20 digits.

LDN: Local dialing number, a string of 1 to 30 digits.

Description Use the **isdn spid1** command to configure SPID information for the B1 channel on the NI-compliant BRI interface.

Use the **undo isdn spid1** command to remove the SPID information of the B1 channel on the interface.

On a BRI interface compliant with the ISDN protocol (North America), calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. By default, dynamic negotiation. Only after SPID information is configured for the B1 channel on the BRI interface can the system makes the L3 initialization to place calls normally.

In addition, when the router works with an ISDN NI compliant switch (the DMS100 for example) in North America, you must use this command to configure a unique SPID and LDN for each B channel to ensure a successful MP channel call. Otherwise, only one B channel can be brought up. Also note that both SPID and LDN are provided by your service provider and the configuration of LDN voids the configuration of the **isdn calling** command.

By default, Both SPID and LDN for the B1 channel on the BRI interface are null.

This command applies only on NI-compliant BRI interfaces.

Example # Set SPID to "012345" for the B1 channel on the interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid1 012345
```

Assign the SPID 012345 and the LDN 54321 to the B1 channel on the BRI 1/0 interface.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid1 012345 54321
```

isdn spid2

Syntax **isdn spid2** *spid* [*LDN*]

undo isdn spid2

View ISDN BRI interface view

Parameter *spid*: String of 1 to 20 digits.

LDN: Local dialing number, a string of 1 to 30 digits.

Description Use the **isdn spid2** command to configure SPID information for the B1 channel on an NI-compliant BRI interface.

Use the **undo isdn spid2** command to remove the SPID information of the B1 channel on the interface.

On a BRI interface compliant with the ISDN protocol in North America, calls can be placed only after the SPID negotiation or initialization is finished. SPID information can be obtained via static configuration or dynamic negotiation. Only after SPID information is configured for the B2 channel on the BRI interface can the system makes the L3 initialization to place calls normally.

In addition, when the router works with an ISDN NI compliant switch (the DMS100 for example) in North America, you must use this command to configure a unique SPID and LDN for each B channel to ensure a successful MP channel call. Otherwise, only one B channel can be brought up. Also note that both SPID and LDN are provided by your service provider and the configuration of LDN voids the configuration of the **ISDN calling** command.

By default, both SPID and LDN for the B2 channel on the BRI interface are null.

This command applies only on NI-compliant BRI interfaces.

Example # Set SPID to "012345" for the B2 channel on the interface BRI 1/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid2 012345
```

Assign the SPID 012345 and the LDN 54321 to the B2 channel on the BRI interface BRI 2/0.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Sysname-Bri1/0] isdn spid2 012345 54321
```

isdn statistics

Syntax **isdn statistics** { **clear** | **continue** | **display** [**flow**] | **start** | **stop** }

View ISDN interface view

Parameter **clear**: Clears the statistics.

continue: Continues counting.

display: Displays the statistics.

display flow: Displays the statistic information about message flows.

start: Starts counting.

stop: Stops counting.

Description Use the **isdn statistics** command to have the system make statistics on the information received and transmitted at an ISDN interface.

By default, no statistics is made on the information transmitted and received at interfaces.

Use the **isdn statistics start** command in the view of an interface to start making statistics on the messages received and transmitted at the interface.

Use the **isdn statistics display** command to view the statistic information.

Use the **isdn statistics continue** command to continue the effort in making statistics.

Use the **isdn statistics display flow** command to view the statistics in the form of flow.

Use the **isdn statistics stop** command to stop making statistics.

Use the **isdn statistics clear** to clear the statistic information.

Example # Start counting incoming and outgoing messages on CE1/PRI interface serial 1/0:15.

```
<Sysname> system-view
[Sysname] interface serial1/0:15
[Sysname-Serial1/0:15] isdn statistics start
```

After a while, stop counting incoming and outgoing messages on CE1/PRI interface serial 1/0:15.

```
[Sysname-Serial1/0:15] isdn statistics stop
```

Display statistics about the received and sent messages forCE1/PRI interface serial 1/0:15.

```
[Sysname-Serial1/0:15] isdn statistics display
Q.931 message received and sent out on current port:
CALL_PROC         Send(0)             Recv(6)
SETUP             Send(6)             Recv(13)
CONN              Send(13)            Recv(5)
SETUP_ACK         Send(0)             Recv(6)
CONNECT_ACK       Send(5)             Recv(13)
DISCONNECT        Send(3)             Recv(16)
RELEASE           Send(1)             Recv(18)
RELEASE_COM       Send(18)            Recv(1)
```

isdn two-tei

Syntax **isdn two-tei**

undo isdn two-tei

View BRI interface view

Parameter None

Description Use the **isdn two-tei** command to have the router requests the connected switch for a new TEI value before calling for a B channel.

Use the **undo isdn two-tei** command to restore the default TEI handling practice on the BRI interface.

This command applies in the situation where the switch with which the router works is an ISDN NI compliant switch (the DMS100 for example) in North America. In this case, you must ensure that the TEI value assigned to each B channel is unique to ensure a successful MP channel call. Otherwise, only one B channel can be brought up and calling for MP fails.

By default, all the B channels on the BRI interface use one TEI value.

Example # Configure the router to request the connected switch for a new TEI value before calling to bring up a B channel.

```
<Sysname> system-view
[Sysname] interface bri 1/0
[Router-Bri1/0] isdn two-tei
```

permanent-active

Syntax **permanent-active**

undo permanent-active

View ISDN BRI interface view

Parameter None

Description Use the **permanent-active** command to specify an ISDN BRI interface to be in permanent active state on physical layer.

Use the **undo permanent-active** command to cancel the configuration.

Note that these two commands are only applicable to ISDN BRI interfaces on BSV boards and operating on network side.

By default, BSV interfaces operating on the network side are not in permanent active state on physical layer.

Note that:

- After you specify a BSV interface operating on the network side to be in permanent active state on physical layer using the **permanent-active** command, no deactivating request is sent to physical layer. In this case, the interface remains in the active state if it is up and the physical link operates smoothly.
- The **permanent-active** command functions differently comparing with the **isdn q921-permanent** command. The former maintains the active state of BRI interfaces on physical layer and is only applicable to BRI interfaces operating on the network side. It cannot activate the BRI interfaces that are in inactive state on physical layer. The latter, however, enables ISDN BRI interfaces operating on user side to set up and maintain Q.921 links automatically. If no Q.921 link is established, the **isdn q921-permanent** command triggers the ISDN BRI interface to establish Q.921 links.

The support for these two commands varies with device models.

Example # Specify BRI 2/0 interface to be in permanent active state on physical layer (assuming that the interface is a BSV interface and operating on network side).

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn protocol-mode network
[Sysname-Bri2/0] permanent-active
```

power-source

Syntax **power-source**

undo power-source

View ISDN BRI interface view

Parameter None

Description Use the **power-source** command to enable remote powering on an ISDN BRI interface.

Use the **undo power-source** command to disable remote powering.

Note that these two commands are only applicable to ISDN BRI interfaces on BSV boards and operating on network side.

By default, remote powering is disabled.

The support for these two commands varies with device models.

Example # Enable remote powering on BRI 2/0 interface (assuming that the interface is a BSV interface and operating on network side).

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname-Bri2/0] isdn protocol-mode network
[Sysname-Bri2/0] power-source
```

shutdown

Syntax **shutdown**

undo shutdown

View ISDN interface view

Parameters None

Description Use the **shutdown** command to shut down an ISDN interface.

Use the **undo shutdown** command to bring up an ISDN interface.

By default, an ISDN interface is up.

Examples # Shut down BRI 2/0.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname- Bri2/0] shutdown
```

Bring up BRI 2/0.

```
<Sysname> system-view
[Sysname] interface bri 2/0
[Sysname- Bri2/0] undo shutdown
```

38 MSTP CONFIGURATION COMMANDS

active region-configuration

Syntax **active region-configuration**

View MST region view

Parameters None

Description Use the **active region-configuration** command to activate your MST region configuration.

When you carry out this command, MSTP will replace the currently running MST region-related parameters with the parameters you have just configured, and will perform spanning tree computing again.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **check region-configuration**.

Examples # Activate MST region configuration manually.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] active region-configuration
```

check region-configuration

Syntax **check region-configuration**

View MST region view

Parameters None

Description Use the **check region-configuration** command to view all the MST region configuration information, including the region name, VLAN-to-instance mapping and revision level settings.

Be sure that your MST region configurations are correct, especially the VLAN-to-instance mapping table. MSTP-compliant devices are in the same MST region only when they have the same region name, the same VLAN-to-instance

mapping table and the same MSTP revision level setting. A device will not be in a different region if it is different in any of these three settings. You can view all the MST region-related configuration information by using this command and determine the MST region the device is currently in, or check whether the MST region configuration is correct.

Related commands: **instance**, **region-name**, **revision-level**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # View all the configuration information of the MST region

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] check region-configuration
Admin Configuration
   Format selector :0
   Region name     :00b010000001
   Revision level  :0

   Instance   Vlans Mapped
      0       1 to 9, 11 to 4094
     15       10
```

Table 102 Description on the fields of the check region-configuration command

Field	Description
Format selector	Configuration format selector of the MST region
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-instance mappings in the MST region

display stp

Syntax **display stp** [**instance** *instance-id*] [**interface** *interface-list*] [**brief**]

View Any view

Parameters **instance** *instance-id*: Displays the spanning tree information of a particular MST instance. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* is 15.

interface *interface-list*: Displays the spanning tree information on one or multiple ports. You can provide up to 10 port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end port number must be greater than the start port number.

brief: Displays brief information.

Description Use the **display stp** command to view the MSTP status information and statistics information.

Based on the MSTP status information and statistics information, you can analyze and maintain the network topology or check whether MSTP is working normally.

Note that:

- If you do not specify any MST instance ID or port list, this command will display the MSTP information on all ports. The displayed information is sequenced by MST instance ID and by port name in each MST instance.
- If you specify an MST instance ID, this command will display the MSTP information on all ports in that MST instance. The displayed information is sequenced by port name.
- If you specify a port list, this command will display the MSTP information on the specified ports. The displayed information is sequenced by MST instance ID, and by port name in each MST instance.
- If you specify both an MST instance ID and a port list, this command will display the MSTP information of the specified MST instance on the specified ports.

The MSTP status information includes:

- CIST global parameters: Protocol work mode, device priority in the CIST instance (Priority), MAC address, hello time, max age, forward delay, maximum hops, common root of the CIST, external path cost from the device to the CIST common root, regional root, the internal path cost from the device to the regional root, CIST root port of the device, and status of the BPDU guard function (enabled or disabled).
- CIST port parameters: Port status, role, priority, path cost, designated bridge, designated port, edge port/non-edge port, whether connecting to a point-to-point link, maximum transmission rate (transmit limit), status of the root guard function (enabled or disabled), BPDU format, boundary port/non-boundary port, hello time, max age, forward delay, message age, remaining hops, whether a port in an aggregation group, and whether rapid state transition enabled (designated ports).
- MSTI global parameters: MSTI instance ID, bridge priority of the instance, regional root, internal path cost, MSTI root port, and master bridge.
- MSTI port parameters: Port status, role, priority, path cost, designated bridge, designated port, remaining hops, whether a port in an aggregation group, and whether rapid state transition enabled (for designated ports).

The statistics information includes:

- The number of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent from each port
- The number of TCN BPDUs, configuration BPDUs, RST BPDUs, MST BPDUs and wrong BPDUs received on each port
- The number of BPDUs discarded on each port

Related commands: **reset stp**.

Examples # View the MSTP status information and statistics information.

```
<Sysname> display stp instance 0 interface Ethernet 1/1 to Ethernet
1/4 GigabitEthernet 1/1 to GigabitEthernet 1/4 brief
  MSTID      Port                  Role  STP State     Protection
    0     Ethernet1/1              ALTE  DISCARDING      LOOP
    0     Ethernet1/2              DESI  FORWARDING      NONE
    0     Ethernet1/3              DESI  FORWARDING      NONE
    0     Ethernet1/4              DESI  FORWARDING      NONE
    0     GigabitEthernet1/1       DESI  FORWARDING      NONE
    0     GigabitEthernet1/2       DESI  FORWARDING      NONE
    0     GigabitEthernet1/3       DESI  FORWARDING      NONE
    0     GigabitEthernet1/4*      DESI  FORWARDING      NONE
  (*) means port in aggregation group
```

Table 103 Description on the fields of the display stp command

Field	Description
MSTID	MST instance ID in the MST region
Port	Port name, corresponding to each MST instance
Role	Port role
STP State	MSTP status on the port, including forwarding, discarding, and learning
Protection	Protection type on the port, including root guard, loop guard, and BPDU guard
(*) means port in aggregation group	* indicates a port in an aggregation group

display stp abnormal-port

Syntax **display stp abnormal-port**

View Any view

Parameters None

Description Use the **display stp abnormal-port** command to view the information about abnormally blocked ports.

Any of the following reasons may cause a port to be abnormally blocked:

- Root guard action
- Loop guard action
- MSTP BPDU format compatibility protection action

Examples # View information about abnormally blocked ports.

```
<Sysname> display stp abnormal-port
MSTID       Blocked Port                    Reason
1           Ethernet1/0                  ROOT-Protected
2           Ethernet1/1                  LOOP-Protected
2           Ethernet1/2                  Formatcompatibility-Protected
```

Table 104 Description on the fields of the display stp abnormal-port command

Field	Description
MSTID	MST instance ID
Blocked Port	Name of blocked port, which corresponds to the related MST instance
Reason	Reason that caused abnormal blocking of the port. ■ ROOT-Protected: root guard action ■ LOOP-Protected: loop guard action ■ Formatcompatibility-Protected: MSTP BPDU format compatibility protection action

display stp down-port

Syntax **display stp down-port**

View Any view

Parameters None

Description Use the **display stp down-port** command to view the information about ports blocked by STP protection actions.

These actions include:

- BPDU attack guard action
- MSTP BPDU format compatibility protection action

Examples # View the information about ports blocked by STP protection actions.

```
<Sysname> display stp down-port
Down Port                Reason
Ethernet1/0          BPDU-Protected
Ethernet1/1          Formatfrequency-Protected
```

Table 105 Description on the fields of the display stp abnormal-port command

Field	Description
Down Port	Name of blocked port
Reason	Reason that caused the port to be blocked. ■ BPDU-Protected: BPDU attack guard action ■ Formatfrequency-Protected: MSTP BPDU format compatibility protection action

display stp history

Syntax **display stp** [**instance** *instance-id*] **history**

View Any view

Parameters **instance** *instance-id*: Displays the historic port role calculation information of a particular spanning tree instance. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* depends on device model.

Description Use the **display stp history** command to view the historic port role calculation information of the specified spanning tree instance or all spanning tree instances.

Note that:

- If you do not specify a spanning tree instance ID, this command will display the historic port role calculation information of all spanning tree instances. The displayed information is sequenced by instance ID, and in the timing of port role calculation in each instance.
- If you specify a spanning tree instance ID, this command will display the historic port role calculation information of only this specified spanning instance, in the timing of port role calculation.

Examples # View the historic port role calculation information of the card on slot 1 in MSTP instance 2.

```
<Sysname> display stp instance 2 history slot 1
 --------------- STP slot 1 history trace ---------------
 -------------------  Instance 2   ---------------------
     Port Ethernet1/1
       Role change   : ROOT->DESI (Aged)
       Time          : 2006/08/08 00:22:56
       Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.1

     Port Ethernet1/2
       Role change   : ALTER->ROOT
       Time          : 2006/08/08 00:22:56
       Port priority : 0.00e0-fc01-6510 0 0.00e0-fc01-6510 128.2
```

Table 106 Description on the fields of the display stp history command

Field	Description
Port	Port name
Role change	A role change of the port (**Aged** means that the change was caused by expiry of a configuration BPDU.)
Time	Time of port role calculation
Port priority	Port priority

display stp region-configuration

Syntax **display stp region-configuration**

View Any view

Parameters None

Description Use the **display stp region-configuration** command to view the currently effective configuration information of the MST region, including the region name, revision level, and user-configured VLAN-to-instance mappings.

Related commands: **stp region-configuration**.

Examples # View the currently effective MST region configuration information.

```
<Sysname> display stp region-configuration
Oper Configuration
   Format selector :0
   Region name     :hello
   Revision level  :0

   Instance   Vlans Mapped
      0       21 to 4094
      1       1 to 10
      2       11 to 20
```

Table 107 Description on the fields of the display stp region-configuration command

Field	Description
Format selector	MSTP-defined format selector
Region name	MST region name
Revision level	Revision level of the MST region
Instance Vlans Mapped	VLAN-to-instance mappings in the MST region

display stp root

Syntax **display stp root**

View Any view

Parameters None

Description Use the **display stp root** command to view the root bridge information of all MSTP instances.

Examples # View the root bridge information of all MSTP instances.

```
<Sysname> display stp root
MSTID    Root Bridge ID       ExtPathCost   IntPathCost     Root Port
0        0.0013.1923.da80         0              0
```

Table 108 Description on the fields of the display stp root command

Field	Description
MSTID	MST instance ID
Root Bridge ID	Root bridge ID
ExtPathCost	External path cost
IntPathCost	Internal path cost

Table 108 Description on the fields of the display stp root command

Field	Description
Root Port	Root port name (displayed only if a port of the current device is the root port of multiple instances)

display stp tc

Syntax **display stp** [**instance** *instance-id*] **tc**

View Any view

Parameters **instance** *instance-id*: Displays the statistics of TC BPDUs (also known as TCN BPDUs) received and sent by all ports in a particular spanning tree instance. The minimum value of *instance-id* is 0, representing the common internal spanning tree (CIST), and the maximum value of *instance-id* depends on the specific device model.

Description Use the **display stp tc** command to view the statistics of TC BPDUs received and sent.

Note that:

- If you do not specify a spanning tree instance ID, this command will display the statistics of TC BPDUs received and sent by all ports in all spanning trees. The displayed information is sequenced by instance ID and by port name in each spanning tree instance.
- If you specify a spanning tree instance ID, this command will display the statistics of TC BPDUs received and sent by all ports in the specified spanning tree instance, in port name order.

Examples # View the statistics of TC BPDUs received and sent by all ports on the card on slot 1 in MSTP instance 0.

```
<Sysname> display stp instance 0 tc slot 1
 -------------- STP slot 1 TC or TCN count -------------
 MSTID      Port                        Receive      Send
   0        Ethernet1/1                   6          4
   0        Ethernet1/2                   0          2
```

Table 109 Description on the fields of the display stp tc command

Field	Description
MSTID	MSTP instance ID in the MST region
Port	Port name
Receive	Number of TC BPDUs received on each port
Send	Number of TC BPDUs received by each port

instance

Syntax **instance** *instance-id* **vlan** *vlan-list*

undo instance *instance-id* [**vlan** *vlan-list*]

View MST region view

Parameters *instance-id*: MST instance ID, in the range of 0 to 15.

vlan-list: VLAN list. You can specify multiple VLANs or VLAN ranges by providing this argument in the form of *vlan-list* = { *vlan-id* [**to** *vlan-id*] }&<1-10>, where, *vlan-id* is in the range of 1 to 4094, and &<1-10> means that you can specify up to 10 VLANs or VLAN ranges for this argument.

Description Use the **instance** command to map the specified VLAN(s) to the specified MST instance.

Use the **undo instance** command to remove the specified VLAN(s) from the specified MST instance and map the removed VLAN(s) to the CIST (MST instance 0).

By default, all VLANs are mapped to the CIST.

Notice that:

- If you specify no VLAN in the **undo instance** command, all VLANs mapped to the specified MST instance will be remapped to the CIST.
- You cannot map the same VLAN to different MST instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.

Related commands: **region-name**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Map VLAN 2 to MST instance 1.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] instance 1 vlan 2
```

region-name

Syntax **region-name** *name*

undo region-name

View MST region view

Parameters *name*: Name of the MST regions, a string of 1 to 32 characters.

Description Use the **region-name** command to configure the MST region name of your device.

Use the **undo region-name** command to restore the MST region name to the default setting.

By default, the MST region name of a device is its MAC address.

The MST region name, the VLAN-to-instance mapping table and the MSTP revision level of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **revision-level**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Set the MST region name of the device to "hello".

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] region-name hello
```

reset stp

Syntax **reset stp** [**interface** *interface-list*]

View User view

Parameters **interface** *interface-list*: Clears the spanning tree statistics information on one or multiple ports. You can provide up to 10 port lists, by each of which you can specify an individual port in the form of *interface-type interface-number*, or a port range in the form of *interface-type start-interface-number* **to** *interface-type end-interface-number*, where the end port number must be greater than the start port number.

Description Use the **reset stp** command to clear the MSTP statistics information.

The MSTP statistics information includes the numbers of TCN BPDUs, configuration BPDUs, RST BPDUs and MST BPDUs sent/received through the specified port(s) (STP BPDUs and TCN BPDUs are counted only for the CIST).

This command clears the spanning tree-related statistics information on the specified port(s) if you specify the *interface-list* argument; otherwise, this command clears the spanning tree-related statistics on all ports.

Related commands: **display stp**.

Examples # Clear the spanning tree-related statistics information on ports Ethernet 1/1 through Ethernet 1/3.

```
<Sysname> reset stp interface Ethernet 1/1 to Ethernet 1/3
```

revision-level

Syntax **revision-level** *level*

undo revision-level

View MST region view

Parameters *level*: MSTP revision level, in the range of 0 to 65535. The system default is 0.

Description Use the **region-level** command to configure the MSTP revision level of your device.

Use the **undo region-level** command to restore the MSTP revision level to the default setting.

The MSTP revision level, the MST region name and the VLAN-to-instance mapping table of a device jointly determine the MST region the device belongs to.

Related commands: **instance**, **region-name**, **check region-configuration**, **vlan-mapping modulo**, and **active region-configuration**.

Examples # Set the MSTP revision level of the MST region to 5.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] revision-level 5
```

stp

Syntax **stp** { **enable** | **disable** }

undo stp

View System view, Ethernet interface view, port group view

Parameters **enable**: Enables the MSTP feature.

disable: Disables the MSTP feature.

Description Use the **stp** command to enable or disable the MSTP feature globally or for a port or a group of ports.

Use the **undo stp** command to restore the default MSTP status globally or for a port or a group of ports.

By default, MSTP is enabled for all ports, and disabled globally.

Note that:

- Configured in system view, the setting is effective for the device globally; configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- To control MSTP flexibly, you can disable the MSTP feature for certain ports so that they will not take part in spanning tree computing and thus to save the device's CPU resources.
- After you enable MSTP, the device determines whether to work in STP-compatible mode, in RSTP mode or in MSTP mode according to your MSTP work mode setting. After MSTP is disabled, the device becomes a transparent bridge.
- After being enabled, MSTP dynamically maintains spanning tree status of the corresponding VLANs based the received configuration BPDUs. After being disabled, it stops maintaining the spanning tree status.
- Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

Related commands: **stp mode**.

Examples # Enable the MSTP feature globally.

```
<Sysname> system-view
[Sysname] stp enable
```

Disable MSTP on port Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] stp disable
```

stp bpdu-protection

Syntax **stp bpdu-protection**

undo stp bpdu-protection

View System view

Parameters None

Description Use the **stp bpdu-protection** command to enable the BPDU guard function for the device.

Use the **undo stp bpdu-protection** command to disable the BPDU guard function for the device.

By default, the BPDU guard function is disabled.

Examples # Enable the BPDU guard function for the device.

```
<Sysname> system-view
[Sysname] stp bpdu-protection
```

stp bridge-diameter

Syntax **stp bridge-diameter** *bridge-number*

undo stp bridge-diameter

View System view

Parameters *bridge-number*: Specifies the switched network diameter, in the range of 2 to 7.

Description Use the **stp bridge-diameter** command to specify the network diameter, namely the maximum number of stations between any two terminal devices on the switched network.

Use the **undo stp bridge-diameter** command to restore the default network diameter setting.

By default, the network diameter of the switched network is 7.

An appropriate setting of hello time, forward delay and max age can speed up network convergence. The values of these timers are related to the network size. You can set these three timers indirectly by setting the network diameter. Based on the network diameter you configured, MSTP automatically sets an optimal hello time, forward delay, and max age for the device. With the network diameter set to 7 (the default), the three timer are also set to their defaults.

Note that this configuration is effective for the CIST and root bridge only, and not for MSTIs.

Related commands: **stp timer forward-delay**, **stp timer hello**, and **stp timer max-age**.

Examples # Set the network diameter of the switched network to 5.

```
<Sysname> system-view
[Sysname] stp bridge-diameter 5
```

stp compliance

Syntax **stp compliance** { **auto | dot1s | legacy** }

undo stp compliance

View Ethernet interface view, port group view

Parameters **auto**: Configures the port(s) to recognize the MSTP BPDU format automatically and accordingly determine the format of MSTP BPDUs to send.

dot1s: Configures the port(s) to receive and send only standard-format (802.1s-compliant) MSTP BPDUs.

legacy: Configures the port(s) to receive and send only compatible-format MSTP BPDUs.

Description Use the **stp compliance** command to configure the mode the port(s) will use to recognize and send MSTP BPDUs.

Use the **undo stp compliance** command to restore the default.

The default mode is **auto**, namely all ports recognize the BPDU format automatically.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- If the mode is set to **auto** on a port, the port automatically recognizes and resolves the received compatible-format BPDUs or 802.1s-compliant BPDUs, and sends, when needed, compatible-format or 802.1s-compliant BPDUs.
- If the mode is set to **legacy** or **dot1s**, on a port, the port can only receive and send BPDUs of the specified format. If the port is configured not to detect the packet format automatically while it works in the MSTP mode, and if it receives a packet in the format other than as configured, that port will become a designated port, and the port will remain in the discarding state to prevent the occurrence of a loop.

Examples # Configure Ethernet 1/1 to receive and send only standard-format (802.1s) MSTP packets.

```
<Sysname>system-view
[Sysname-Ethernet1/1] stp compliance dot1s
```

Restore the default mode for port Ethernet 1/1 to recognize and send MSTP BPDUs.

```
[Sysname-Ethernet1/1] undo stp compliance
```

stp config-digest-snooping

Syntax **stp config-digest-snooping**

undo stp config-digest-snooping

View System view, Ethernet interface view, port group view

Parameters None

Description Use the **stp config-digest-snooping** command to enable Digest Snooping.

Use the **undo stp config-digest-snooping** command to disable Digest Snooping.

The feature is disabled by default.

Notice that:

- You need to enable this feature both globally and on ports connected to other vendors' devices to make it take effect. It is recommended to enable the feature on all associated ports first and then globally, making all configured ports take effect at the same time to minimize the impact, and disable the feature globally to disable it on all associated ports.
- It is not recommended to enable Digest Snooping on the MST region edge port to avoid loops.
- Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

Examples # Enable global Digest Snooping.

```
<Sysname> system-view
[Sysname] stp config-digest-snooping
```

Enable Digest Snooping on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] stp config-digest-snooping
```

stp cost

Syntax **stp** [**instance** *instance-id*] **cost** *cost*

undo stp [**instance** *instance-id*] **cost**

View Ethernet interface view, port group view

Parameters **instance** *instance-id*: Sets the path cost of the port(s) in a particular MST instance. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 15.

cost: Path cost of the port, the effective range of which depends on the path cost calculation standard adopted.

Description Use the **stp cost** command to set the path cost of the port(s) in the specified MST instance or all MST instances.

Use the **undo stp cost** command to restore the default.

By default, the device automatically calculates the path costs of ports in each MST instance based on the corresponding standard.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- If you set *instance-id* to 0, you are setting the path cost of the port in the CIST. The path cost setting of a port can affect the role selection of the port. Setting different path costs for the same port in different MST instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing. When the path cost of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the path cost of port Ethernet 1/3 in MST instance 2 to 200.

```
<Sysname> system-view
[Sysname] interface ethernet 1/3
[Sysname-Ethernet1/3] stp instance 2 cost 200
```

stp edged-port

Syntax **stp edged-port** { **enable** | **disable** }

undo stp edged-port

View Ethernet interface view, port group view

Parameters **enable**: Configures the current port to be an edge port.

disable: Configures the current port to be a non-edge port.

Description Use the **stp edged-port enable** command to configure the current port to be an edge port.

Use the **stp edged-port disable** or **undo stp edged-port enable** command to configure the current port to be a non-edge port.

All Ethernet ports are non-edge ports by default.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- If a port directly connects to a user terminal rather than another device or a shared LAN segment, this port is regarded as an edge port. When the network topology changes, an edge port will not cause a temporary loop. Therefore, configuring a port as an edge port can enable the port to transition to the forwarding state rapidly. We recommend that you configure an Ethernet port directly connecting to a user terminal as an edge port before to enable it to transition to the forwarding state rapidly.

- Normally, configuration BPDUs from other devices cannot reach an edge port because it does not connect to any other device. Before the BPDU guard function is enabled, if a port receives a configuration BPDU, the port is working actually as a non-edge port even if you have configured in as an edge port.

Examples # Configure port Ethernet 1/1 as a non-edge port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] stp edged-port disable
```

stp loop-protection

Syntax **stp loop-protection**

undo stp loop-protection

View Ethernet interface view, port group view

Parameters None

Description Use the **stp loop-protection** command to enable the loop guard function for a port or a group of ports.

Use the **undo stp loop-protection** command to restore default loop guard setting for a port of a group of ports.

By default, the loop guard function is disabled.

Note that, configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.

Examples # Enable the loop guard function for port Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] stp loop-protection
```

stp max-hops

Syntax **stp max-hops** *hops*

undo stp max-hops

View System view

Parameters *hops*: Maximum hops, in the range of 1 to 40

Description Use the **stp max-hops** command to set the maximum hops of the MST region on the device.

Use the **undo stp max-hops** command to restore the maximum hops to the default setting.

By default, the maximum hops of an MST region is 20.

In the CIST and MST instances, the maximum hops setting configured on the regional root bridge determines the maximum network diameter supported by the MST region. After a configuration BPDU leaves the root bridge, its hop count is decremented by 1 whenever it passes a device. When its hop count reaches 0, it will be discarded by the device that has received it. As a result, devices beyond the maximum hop count are unable to take part in spanning tree computing, and thereby the size of the MST region is limited.

When the current device becomes the root bridge of the CIST or an MSTI, the maximum hops setting configured on the device becomes the network diameter of that spanning tree and restricts the size of that spanning tree in the current MST region.

Devices other than the root bridge in an MST region use the maximum hops setting on the root bridge.

Examples # Set the maximum hops of the MST region to 35.

```
<Sysname> system-view
[Sysname] stp max-hops 35
```

stp mcheck

Syntax **stp mcheck**

View System view/Ethernet interface view

Parameters None

Description Use the **stp mcheck** command to carry out the mCheck operation globally or on a port.

In a switched network, if a port on the device running MSTP (or RSTP) connects to a device running STP, this port will automatically migrate to the STP-compatible mode. However, if the device running STP is removed, this will not be able to migrate automatically to the MSTP (or RSTP) mode, but will remain working in the STP-compatible mode. In this case, you can perform an mCheck operation to force the port to migrate to the MSTP (or RSTP) mode.

Note that the **stp mcheck** command is meaningful only when the device works in the MSTP (or RSTP) mode, not in the STP-compatible mode.

Related commands: **stp mode**.

Examples # Carry out mCheck on port Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/1
[Sysname-Ethernet1/1] stp mcheck
```

stp mode

Syntax **stp mode** { **stp** | **rstp** | **mstp** }

undo stp mode

View System view

Parameters **stp**: Configures the MSTP-compliant device to work in STP-compatible mode.

rstp: Configures MSTP-compliant device to work in RSTP mode.

mstp: Configures MSTP-compliant device to work in MSTP mode.

Description Use the **stp mode** command to configure the MSTP work mode of the device.

Use the **undo stp mode** command to restore the MSTP work mode to the default setting.

By default, an MSTP-compliant device works in MSTP mode.

Related commands: **stp mcheck**, **stp**.

Examples # Configure the MSTP-compliant device to work in STP-compatible mode.

```
<Sysname> system-view
[Sysname] stp mode stp
```

stp no-agreement-check

Syntax **stp no-agreement-check**

undo stp no-agreement-check

View Ethernet interface view, port group view

Parameters None

Description Use the **stp no-agreement-check** command to enable No Agreement Check on port(s).

Use the **undo stp no-agreement-check** command to disable No Agreement Check on port(s).

By default, No Agreement Check is disabled.

The No Agreement Check feature can take effect only on the root port or alternate port.

Examples # Enable No Agreement Check on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] stp no-agreement-check
```

stp pathcost-standard

Syntax **stp pathcost-standard** { **dot1d-1998** | **dot1t** | **legacy** }

undo stp pathcost-standard

View System view

Parameters **dot1d-1998**: The device calculates the default path cost for ports based on IEEE 802.1D-1998.

dot1t: The device calculates the default path cost for ports based on IEEE 802.1t.

legacy: The device calculates the default path cost for ports based on a private standard.

Description Use the **stp pathcost-standard** command to specify a standard for the device to use when calculating the default path cost of the link connected with the device

Use the **undo stp pathcost-standard** command to restore the default setting of the calculation standard.

The default standard used by the device is **legacy**.

Note that if you change the standard that the device uses in calculating the default path cost, the port path cost value set through the **stp cost** command will be out of effect.

Table 110 Link speed vs. path cost

Link speed	Duplex state	802.1D-1998	IEEE 802.1t	Private standard
0	-	65535	200,000,000	200,000
10Mbps	Single Port	100	2,000,000	2,000
	Aggregated Link 2 Ports	100	1,000,000	1,800
		100	666,666	1,600
	Aggregated Link 3 Ports	100	500,000	1,400
	Aggregated Link 4 Ports			

Table 110 Link speed vs. path cost

Link speed	Duplex state	802.1D-1998	IEEE 802.1t	Private standard
100Mbps	Single Port	19	200,000	200
	Aggregated Link 2 Ports	19	100,000	180
		19	66,666	160
	Aggregated Link 3 Ports	19	50,000	140
	Aggregated Link 4 Ports			
1000Mbps	Single Port	4	20,000	20
	Aggregated Link 2 Ports	4	10,000	18
		4	6,666	16
	Aggregated Link 3 Ports	4	5,000	14
	Aggregated Link 4 Ports			
10Gbps	Single Port	2	2,000	2
	Aggregated Link 2 Ports	2	1,000	1
		2	666	1
	Aggregated Link 3 Ports	2	500	1
	Aggregated Link 4 Ports			

In the calculation of the path cost value of an aggregated link, 802.1D-1998 does not take into account the number of ports in the aggregated link. Whereas, 802.1T takes the number of ports in the aggregated link into account. The calculation formula is: Path Cost = 200,000,000/link speed (in 100 kbps), where link speed is the sum of the link speed values of the non-blocked ports in the aggregated link.

Examples # Configure the device to calculate the default path cost for ports based on IEEE 802.1D-1998.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1d-1998
```

Configure the device to calculate the default path cost for ports based on IEEE 802.1t.

```
<Sysname> system-view
[Sysname] stp pathcost-standard dot1t
```

stp point-to-point

Syntax **stp point-to-point** { **auto** | **force-false** | **force-true** }

undo stp point-to-point

View Ethernet interface view, port group view

Parameters **auto**: Specifies MSTP detects automatically whether the current port connects to a point-to-point link.

force-false: Specifies the current port to connect to a non-point-to-point link.

force-true: Specifies the current port to connect to a point-to-point link.

Description Use the **stp point-to-point** command to specify whether the current port connects to a point-to-point link.

Use the **undo stp point-to-point** command to restore the default status of the link connected with the current port.

The default setting is **auto**; namely the MSTP-compliant device automatically detects whether an Ethernet port connects to a point-to-point link.

Configured in Ethernet interface view, the setting is effective on the current port only.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- When connecting to a non-point-to-point link, a port is incapable of rapid state transition.
- If the current port is the master port of aggregated ports or if it works in full duplex mode, the link to which the current port connects is a point-to-point link. We recommend that you use the default setting, namely let MSTP detect the link status automatically.
- This setting is effective to the CIST and all MST instances. If a port is configured as connecting to a point-to-point link or a non-point-to-point link, the setting takes effect for the port in all MST instances. If the physical link to which the port connects is not a point-to-point link and you force it to be a point-to-point link by configuration, your configuration may incur a temporary loop.

Examples # Configure port Ethernet 1/3 as connecting to a point-to-point link.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/3
[Sysname-Ethernet1/3] stp point-to-point force-true
```

stp port-log

Syntax **stp port-log** { **all** | **instance** *instance-id* }

undo stp port-log { **all** | **instance** *instance-id* }

View System view

Parameters **all**: Enables output of port state transition information for all instances.

instance *instance-id*: Enables output of port state transition information for the specified instance. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of this argument depends on the specific device model.

Description Use the **stp port-log** command to enable output of port state transition information for the specified instance or all instances.

Use the **undo stp port-log** command to disable output of port state transition information for the specified instance or all instances.

Whether this function is enabled by default depends on the specific device model.

Examples # Enable output of port state transition information for instance 2.

```
<Sysname> system-view
[Sysname] stp port-log instance 2
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PDISC: Instance 2's Etherne
t1/1 has been set to discarding state!
%Aug 16 00:49:41:856 2006 Sysname MSTP/3/PFWD: Instance 2's Ethernet
1/2 has been set to forwarding state!
```

// The information mentioned above shows that in instance 2, that state of both Ethernet 1/1 and Ethernet 1/2 has changed to forwarding.

stp port priority

Syntax **stp** [**instance** *instance-id*] **port priority** *priority*

undo stp [**instance** *instance-id*] **port priority**

View Ethernet interface view, port group view

Parameters **instance** *instance-id*: Sets the priority of the current port(s) in a particular spanning tree instance. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 15.

priority: Port priority, in the range of 0 to 240 at the step of 16 (0, 16, 32..., for example).

Description Use the **stp port priority** command to set the priority of the port(s).

Use the **undo stp port priority** command to restore the default.

By default, the port priority is 128.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.

- If you set *instance-id* to 0, you are setting the priority of the port in the CIST. The priority of a port can affect the role selection of the port in the specified MST instance.
- Setting different priorities for the same port in different MST instances allows different VLAN traffic flows to be forwarded along different physical links, thus to enable per-VLAN load balancing.
- When the priority of a port is changed, MSTP will re-compute the role of the port and initiate a state transition.
- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the priority of port Ethernet 1/3 in MST instance 2 to 16.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/3
[Sysname-Ethernet1/3] stp instance 2 port priority 16
```

stp priority

Syntax **stp** [**instance** *instance-id*] **priority** *priority*

undo stp [**instance** *instance-id*] **priority**

View System view

Parameters **instance** *instance-id*: Sets the priority of the current port(s) in a particular spanning tree instance. The minimum value of *instance-id* is 0, representing the CIST, and the maximum value of *instance-id* is 15.

priority: Port priority, in the range of 0 to 61440 at the step of 4096, namely you can set up to 16 priority values, such as 0, 4096, 8192..., on the device.

Description Use the **stp priority** command to set the priority of the device.

Use the **undo stp priority** command to restore the device priority to the default setting.

By default, the device priority is 32768.

The device priority is involved in spanning tree computing. The device priority is set on a per-instance basis. An MSTP-compliant device can have different priorities in different MST instances.

If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.

Examples # Set the device priority in MST instance 1 to 4096.

```
<Sysname> system-view
[Sysname] stp instance 1 priority 4096
```

stp region-configuration

Syntax **stp region-configuration**

undo stp region-configuration

View System view

Parameters None

Description Use the **stp region-configuration** command to enter MST region view.

Use the **undo stp region-configuration** command to restore the default MST region configurations.

By default, the default settings are used for all the three MST region parameters. Namely, the device's MST region name is the device's MAC address, all VLANs are mapped to the CIST, and the MSTP revision level is 0.

After you enter MST region view, you can configure the parameters related the MST region, including the region name, VLAN-to-instance mapping and revision level.

Examples # Enter MST region view.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region]
```

stp root primary

Syntax **stp** [**instance** *instance-id*] **root primary**

undo stp [**instance** *instance-id*] **root**

View System view

Parameters **instance** *instance-id*: MST instance ID, in the range of 0 to 15. MST instance 0 represents the CIST.

Description Use the **stp root primary** command to specify the current device as the root bridge of the specified MST instance.

Use the **undo stp root** command to remove the current device as the root bridge of the specified MST instance.

By default, a device is not a root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- There is only one root bridge in effect in a spanning tree instance. If two or more devices have been designated to be root bridges of the same spanning tree instance, MSTP will select the device with the lowest MAC address as the root bridge.
- You can specify a root bridge for each MST instance without caring about the device priority. After specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

Examples # Define the current device as the root bridge of MST instance 0.

```
<Sysname> system-view
[Sysname] stp instance 0 root primary
```

stp root secondary

Syntax **stp** [**instance** *instance-id*] **root secondary**

undo stp [**instance** *instance-id*] **root**

View System view

Parameters **instance** *instance-id*: MST instance ID, in the range of 0 to 15. MST instance 0 represents the CIST.

Description Use the **stp root secondary** command to specify the current device as a secondary root bridge of the specified MST instance.

Use the **undo stp root** command to remove the current device as a secondary root bridge of the specified MST instance.

By default, a device is not a secondary root bridge.

Note that:

- If you do not provide **instance** *instance-id*, your configuration will take effect in the CIST instance only.
- You can configure one or more secondary root bridges for each MST instance. When the root bridge of an instance fails or is shut down, the secondary root bridge can take over the role of the instance of the specified MST instance. If you specify more than one secondary root bridge, the secondary root bridge with the lowest Mac address will become the root bridge.
- Upon specifying the current device as the root bridge or a secondary root bridge, you cannot change the priority of the device.

Examples # Define the current device as the secondary root bridge of MST instance 0.

```
<Sysname> system-view
[Sysname] stp instance 0 root secondary
```

stp root-protection

Syntax **stp root-protection**

undo stp root-protection

View Ethernet interface view, port group view

Parameters None

Description Use the **stp root-protection** command to enable the root guard function for a port or a group of ports.

Use the **undo stp root-protection** command to restore default setting of the root guard function for the port(s).

By default, the root guard function is disabled.

Note that, configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.

Examples # Enable the root guard function for port Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/1
[Sysname-Ethernet1/1] stp root-protection
```

stp tc-protection

Syntax **stp tc-protection enable**

stp tc-protection disable

View System view

Parameters None

Description Use the **stp tc-protection enable** command to enable the TC-BPDU attack guard function for the device.

Use the **stp tc-protection disable** command to disable the TC-BPDU attack guard function for the device.

By default, the TC-BPDU attack guard function is enabled.

Examples # Enable the TC-BPDU attack guard function for the device.

```
<Sysname> system-view
[Sysname] stp tc-protection enable
```

stp tc-protection threshold

Syntax **stp tc-protection threshold** *number*

undo stp tc-protection threshold

View System view

Parameters *number*: Maximum number of times the device deletes forwarding address entries within a certain period of time immediately after it receives TC-BPDUs, in the range of 1 to 255.

Description Use the **stp tc-protection threshold** command to configure the maximum number of times the device deletes forwarding address entries within 10 seconds immediately after it receives TC-BPDUs.

Use the **undo stp tc-protection threshold** command to restore the default configuration.

By default, the device limits the maximum number of times of deleting forwarding address entries within a certain period of time immediately after it receives TC-BPDUs to 6 times.

Examples # Set the maximum number of times the device deletes forwarding address entries within a certain period of time immediately after it receives TC-BPDUs to 10.

```
<Sysname> system-view
[Sysname] stp tc-protection threshold 10
```

stp timer forward-delay

Syntax **stp timer forward-delay** *centi-seconds*

undo stp timer forward-delay

View System view

Parameters *centi-seconds*: Forward delay, in the range 400 to 3,000 (in centiseconds). This argument must be a multiple of 100.

Description Use the **stp timer forward-delay** command to set the forward delay timer of the device.

Use the **undo stp timer forward-delay** command to restore the forward delay timer of the device to the default setting.

By default, the forward delay timer is set to 1,500 centiseconds.

In order to prevent temporary loops, a port must go through an intermediate state, the learning state, before it transitions from the discarding state to the

forwarding state, and must wait a certain period of time before it transitions from one state to another to keep synchronized with the remote device during state transition. The forward delay timer set on the root bridge determines the time interval of state transition.

If the current device is the root bridge, the state transition interval of the device depends on the set forward delay value; for a secondary root bridge, its state transition interval is determined by the forward delay timer set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) ƒ max age
- Max age ƒ 2 × (hello Time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp bridge-diameter** *bridge-number* command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer hello**, **stp timer max-age**, and **stp bridge-diameter**.

Examples # Set the forward delay timer of the device to 2,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer forward-delay 2000
```

stp timer hello

Syntax **stp timer hello** *centi-seconds*

undo stp timer hello

View System view

Parameters *centi-seconds*: Hello time, in the range 100 to 1,000 (in centiseconds). This argument must be a multiple of 100.

Description Use the **stp timer hello** command to set the hello time of the device.

Use the **undo stp timer hello** command to restore the hello time of the device to the default setting.

By default, the hello time is set to 200 centiseconds.

Hello time is the time interval at which MSTP-compliant devices send configuration BPDUs to maintain spanning tree stability. If a device fails to receive configuration BPDUs within the set period of time, a new spanning tree computing process will be triggered due to timeout. The root bridge sends configuration BPDUs at the

interval of the hello time set on the device, while secondary root bridges use the hello time set on the root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) ƒ max age
- Max age ƒ 2 × (hello time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter of the switched network in the **stp bridge-diameter** *bridge-number* command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer max-age**, and **stp bridge-diameter**.

Examples # Set the hello time of the device to 400 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer hello 400
```

stp timer max-age

Syntax **stp timer max-age** *centi-seconds*

undo stp timer max-age

View System view

Parameters *centi-seconds*: Max age, in the range 600 to 4,000 (in centiseconds). This argument must be a multiple of 100.

Description Use the **stp timer max-age** command to set the max age timer of the device.

Use the **undo stp timer max-age** command to restore the max age timer of the device to the default setting.

By default, the max age is set to 2,000 centiseconds.

MSTP can detect link faults and automatically restore the forwarding state of the redundant link. In the CIST, the device determines whether a configuration BPDU received on a port has expired based on the max age timer. If a port receives a configuration BPDU that has expired, that MST instance needs to re-computed.

The max age timer is not meaningful for MSTIs. If the current device is the root bridge of the CIST, it determines whether a configuration BPDUs has expired based on the configured max age timer; if the current device is not the root bridge of the CIST, it uses the max age timer set on the CIST root bridge.

The setting of the hello time, forward delay and max age timers must meet the following formulae.

- 2 × (forward delay - 1 second) ƒ max age
- Max age ƒ 2 × (hello time + 1 second)

MSTP can work effectively on the entire network only when the above-mentioned conditions are met; otherwise, network instability will frequently occur. We recommend that you specify the network diameter in the **stp bridge-diameter** *bridge-number* command and let MSTP automatically calculate an optimal setting of these three timers.

Related commands: **stp timer forward-delay**, **stp timer hello**, and **stp bridge-diameter**.

Examples # Set the max age timer of the device to 1,000 centiseconds.

```
<Sysname> system-view
[Sysname] stp timer max-age 1000
```

stp timer-factor

Syntax **stp timer-factor** *number*

undo stp timer-factor

View System view

Parameters *number*: Timeout factor, in the range of 1 to 20.

Description Use the **stp timer-factor** command to configure the timeout time of the device by setting the timeout factor. Timeout time = timeout factor × 3 × hello time.

Use the **undo stp timer-factor** command to restore the timeout factor to the default setting.

By default, the timeout factor of the device is set to 3.

After the network topology is stabilized, each non-root-bridge device forwards configuration BPDUs to the surrounding devices at the interval of hello time to check whether any link is faulty. Typically, if a device does not receive a BPDU from the upstream device within nine times the hello time, it will assume that the upstream device has failed and start a new spanning tree calculation process.

In a very stable network, this kind of spanning tree computing may occur because the upstream device is busy. In this case, you can avoid such unwanted spanning tree computing by lengthening the timeout time (by setting the timeout factor to 4 or more). We recommend that you set the timeout factor to 5, or 6, or 7 for a stable network.

Examples # Set the timeout factor of the device to 7.

```
<Sysname> system-view
[Sysname] stp timer-factor 7
```

stp transmit-limit

Syntax **stp transmit-limit** *packet-number*

undo stp transmit-limit

View Ethernet interface view, port group view

Parameters *packet-number*: Maximum number of MSTP packets that the port can send within each hello time, namely the maximum transmission rate of the port, in the range of 1 to 255.

Description Use the **stp transmit-limit** command to set the maximum transmission rate of a port or a group of ports.

Use the **undo stp transmit-limit** command to restore the maximum transmission rate of a port or a group of ports to the default setting.

By default, the maximum transmission rate of all ports of the device is 10.

Note that:

- Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all the ports in the port group.
- A larger maximum transmission rate value represents more MSTP packets that the port will send within each hello time, but this means that more device resources will be used. An appropriate maximum transmission rate setting can prevent MSTP from using an excessive bandwidth resource during network topology instability.

Examples # Set the maximum transmission rate of port Ethernet 1/1 to 5.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/1
[Sysname-Ethernet1/1] stp transmit-limit 5
```

vlan-mapping modulo

Syntax **vlan-mapping modulo** *modulo*

View MST region view

Parameters *modulo*: Modulo value, in the range of 1 to 15.

Description Use the **vlan-mapping modulo** command to map VLANs in the current MST region to MST instances according to the specified modulo value.

By default, all VLANs are mapped to the CIST (instance 0).

You cannot map the same VLAN to different MST instances. If you map a VLAN that has been mapped to an instance to a new instance, the old mapping will be automatically removed.

*By using the **vlan-mapping modulo** command, you can quickly specify a VLAN for each MST instance. This command maps each VLAN to the MST instance whose ID is (VLAN ID-1) %modulo + 1, where (VLAN ID-1) %modulo is the modulo operation for (VLAN ID-1). If the modulo value is 15, for example, then VLAN 1 will be mapped to MSTI 1, VLAN 2 to MSTI 2, VLAN 16 to MSTI 1, VLAN 17 to MSTI 2, and so on.*

Related commands: **region-name**, **revision-level**, **check region-configuration**, and **active region-configuration**.

Examples # Map VLANs to MSTIs as per the modulo value of 8.

```
<Sysname> system-view
[Sysname] stp region-configuration
[Sysname-mst-region] vlan-mapping modulo 8
```

39 VLAN CONFIGURATION COMMANDS

description

Syntax **description** *text*

undo description

View VLAN view/VLAN interface view

Parameter *text*: A string that describes the current VLAN or VLAN interface (Space can be included), case sensitive.

- For VLAN, this is a string of 1 to 32 characters.
- For VLAN interface, this is a string of 1 to 80 characters.

Description Use the **description** command to configure the descriptive string of the current VLAN or VLAN interface.

Use the **undo description** command to restore the default.

By default, the descriptive string for a VLAN is the VLAN ID, for example, "VLAN 0001"; for a VLAN interface is name of the current VLAN interface, for example, "Vlan-interface1 Interface"

Example # Assign a descriptive string "RESEARCH" for VLAN 1.

```
<Sysname> system-view
[Sysname] vlan 1
[Sysname-vlan1] description RESEARCH
```

Assign a descriptive string "VLAN-INTERFACE-2" for VLAN interface 2

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] description VLAN-INTERFACE-2
```

display interface vlan-interface

Syntax **display interface vlan-interface** [*vlan-interface-id*]

View Any view

Parameter *vlan-interface-id*: VLAN interface ID.

Description Use the **display interface vlan-interface** command to display the relevant information of a VLAN interface.

Execution of the command with the parameter included will display the information of a specified VLAN interface; otherwise, information on all created VLAN interfaces will be displayed.

Related command: **interface vlan-interface**.

Example # Display the information of VLAN-interface 2.

```
<Sysname> display interface vlan-interface 2
Vlan-interface2 current state: DOWN
Line protocol current state: DOWN
Description: Vlan-interface2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 00e0-fc00-0001
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 00e0-fc00-0001
Last 300 seconds input:  0 bytes/sec 0 packets/sec
Last 300 seconds output:  0 bytes/sec 0 packets/sec
     0 packets input, 0 bytes, 0 drops
     0 packets output, 0 bytes, 0 drops
```

Table 111 Description on the fields of the display interface vlan-interface command

Field	Description
Vlan-interface2 current state	The physical state of a VLAN interface
Line protocol current state	The link layer protocol state of a VLAN interface
Description	The description of a VLAN interface
The Maximum Transmit Unit	The MTU of a VLAN interface
Internet protocol processing :	IP processing ability
IP Packet Frame Type	IPv4 outgoing frame format
Hardware address	MAC address corresponding to a VLAN interface
IPv6 Packet Frame Type	IPv6 outgoing frame format
Last 300 seconds input: 0 bytes/sec 0 packets/sec Last 300 seconds output: 0 bytes/sec 0 packets/sec	Average rate of input packets and output packets in the last 300 seconds (in bps)
0 packets input, 0 bytes, 0 drops	Total number and size (in bytes) of the received packets of the interface and the number of the dropped packets
0 packets output, 0 bytes, 0 drops	Total number and size (in bytes) of the transmitted packets of the interface and the number of the dropped packets

display vlan

Syntax **display vlan** [*vlan-id1* [**to** *vlan-id2*] | **all** | **dynamic** | **interface** *interface-type interface-number.subnumber* | **reserved** | **static**]

View Any view

Parameter *vlan-id1*: Displays the information of a VLAN specified by VLAN ID in the range of 1 to 4,094.

vlan-id1 **to** *vlan-id2*: Displays the information of a range of VLANs specified by a VLAN ID range.

all: Displays all current VLAN information except for the reserved VLAN.

dynamic: Displays the information of dynamically VLANs

interface *interface-type interface-number.subnumber*: Displays VLAN information on a specified sub-interface. The *interface-type interface-number.subnumber* parameters specify the interface type and interface number, in which *interface-number* is the main interface number whereas *subnumber* is the sub-interface number, ranging from 1 to 4,094.

reserved: Displays information of the reserved VLANs. Protocol modules determine reserved VLANs according to function implementation, and reserved VLANs serve protocol modules. Reserved VLANs cannot be modified.

static: Displays static VLAN information.

Description Use the **display vlan** command to display VLAN information.

Related command: **vlan**.

Example # Display VLAN 2 information.

```
<Sysname> display vlan 2
VLAN ID: 2
 VLAN Type: static
 Route interface: not configured
 Description: VLAN 0002
Broadcast MAX-ratio: 100%
Tagged   Ports: none
 Untagged Ports:
Ethernet1/1  Ethernet1/2  Ethernet1/3
```

Display VLAN 3 information.

```
<Sysname> display vlan 3
 VLAN ID: 3
 VLAN Type: static
 Route Interface: configured
 IP Address: 1.1.1.1
 Subnet Mask: 255.255.255.0
```

```
Description: VLAN 0003
Tagged   Ports: none
Untagged Ports: none
```

Table 112 Description on the fields of the display vlan command

Field	Description
VLAN ID	VLAN ID
VLAN Type	VLAN type (static or dynamic)
Route interface	Whether the VLAN interface is configured for the VLAN: not configured or configured
Description	VLAN descriptive string
Broadcast MAX-ratio	VLAN broadcast suppression ratio (available only on the device supporting the **broadcast-suppression** command)
IP Address	IP address of the VLAN interface (not display if the VLAN interface has no IP address configured)
Subnet Mask	Subnet mask of the IP address (not display if the VLAN interface has no IP address configured)
Tagged Ports	Tagged ports
Untagged Ports	Untagged ports

interface vlan-interface

Syntax **interface vlan-interface** *vlan-interface-id*

undo interface vlan-interface *vlan-interface-id*

View System view

Parameter *vlan-interface-id*: VLAN interface ID, in the range of 1 to 4,094.

Description Use the **interface vlan-interface** command to enter the specified VLAN interface view. Use the **undo interface vlan-interface** command to delete the specified VLAN interface. The VLAN interface must be created first before entering its view

Before creating a VLAN interface, make sure the corresponding VLAN has been created; otherwise, the VLAN interface cannot be created.

Related command: **display interface vlan-interface**.

Example # Create VLAN interface 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] quit
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2]
```

ip address

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View VLAN interface view

Parameter *ip-address*: IP address of a VLAN interface, in dotted decimal format.

mask: Subnet mask that corresponds to the IP address of a VLAN interface, in dotted decimal format.

mask-length: Length of a sub-net mask, indicated by the number of "1"s, in the range 0 to 32.

sub: Indicates the address is a sub-IP address of the VLAN interface.

Description Use the **ip address** command to specify the IP address and subnet mask for a VLAN interface.

Use the **undo ip address** command to remove the IP address and sub-net mask for a VLAN interface.

By default, no IP address is configured.

An interface normally has one IP address. To enable a device to connect to multiple subnets, a maximum of 32 IP addresses can be configured on a VLAN interface, in which one is the primary IP address and all the rest are secondary IP addresses. The total number of IP addresses on a VLAN interface varies by device. Their relationship is illustrated as follows:

- A newly configured main IP address will replace the original one, if there is one.
- Using the **undo ip address** command without any parameter indicates that all IP addresses will be deleted from the VLAN interface.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to delete the main IP address.
- Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to delete a sub-interface.
- Note that before deletion of the main IP address you must first delete the sub-IP address.

Related command: **display ip interface** on page 781.

Example # Specify the IP address as 1.1.0.1, the sub-net mask as 255.255.255.0 for the VLAN interface 1.

```
<Sysname> system-view
[Sysname] interface vlan-interface 1
[Sysname-Vlan-interface1] ip address 1.1.0.1 255.255.255.0
```

shutdown

Syntax **shutdown**

undo shutdown

View VLAN interface view

Parameter None

Description Use the **shutdown** command to shut down a VLAN interface.

Use the **undo shutdown** command to bring up a VLAN interface.

By default, the VLAN interface is down if all ports in the VLAN are down, as long as one port in the VLAN is up, the VLAN interface will be up

You can use the **undo shutdown** command to bring up a VLAN interface after configurations of the related parameter and protocol. When there is a fault in a VLAN interface, you can use the **shutdown** command to shut down the interface and then bring it up using the **undo shutdown** command. In this way, the interface will resume Shutting down/bringing up a VLAN interface does not affect any Ethernet ports in the VLAN. The state of an Ethernet port does not change with the VLAN interface state.

Example # Shut down the VLAN interface and then bring it up.

```
<Sysname> system-view
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] shutdown
[Sysname-Vlan-interface2] undo shutdown
```

vlan

Syntax **vlan** { *vlan-id1* [**to** *vlan-id2*] | **all** }

undo vlan { *vlan-id1* [**to** *vlan-id2*] | **all** }

View System view

Parameter *vlan-id1*: VLAN ID, in the range of 1 to 4,094.

vlan-id1 **to** *vlan-id2*: Specifies a VLAN range. Both the *vlan-id1* argument and the *vlan-id2* argument are in the range of 1 to 4094.

all: Creates or deletes all VLANs except reserved VLANs. The keyword is not supported when the number of maximum VLANs that can be created on a device is less than 4094.

Description Use the **vlan** *vlan-id* command to create specified VLAN(s).

If a specified VLAN exists, the command places you into its view.

Use the **undo vlan** command to delete specified VLAN(s).

Note that:

- As the default VLAN, VLAN 1 cannot be created or removed.
- You cannot create/remove reserved VLANs that are reserved for specific function implementation.
- Dynamic VLANs cannot be removed using the **undo vlan** command.
- A VLAN associated with QoS policies cannot be removed.

Related command: **display vlan**.

Example # Enter VLAN 2 view.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2]
```

Create VLAN 4 through VLAN 100.

```
<Sysname> system-view
[Sysname] vlan 4 to 100
Please wait.............. Done.
```

40 PORT-BASED VLAN CONFIGURATION COMMANDS

port

Syntax **port** *interface-list*

undo port *interface-list*

View VLAN interface view

Parameter **interface** *interface-list*: Ethernet interface list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> means that you can specify up to 10 port ranges.

Description Use the **port** command to add one Access port or a group of Access ports to a VLAN. Use the **undo port** command to remove one Access port or a group of Access ports from a VLAN.

Note:

- This command is only applicable to Access ports.
- All ports have their default link type configured as Access, however, users can manually configure the port type. For more information, refer to "port link-type" on page 642.

Related command: **display vlan**.

Example # Add the ports from Ethernet 1/1 to Ethernet 1/3 to VLAN 2.

```
<Sysname> system-view
[Sysname] vlan 2
[Sysname-vlan2] port ethernet 1/1 to ethernet 1/3
```

port access vlan

Syntax **port access vlan** *vlan-id*

undo port access vlan

View Ethernet interface view, port group view

Parameter *vlan-id* : VLAN ID, in the range 1 to 4094.

Description Use the **port access vlan** command to add the current Access port to a specified VLAN.

Use the **undo port access vlan** command to add the current Access port to the default VLAN.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group. Make sure that the VLAN identified by the *vlan-id* argument exists before issuing the **port access vlan** command.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

Example # Add Ethernet 1/1 to VLAN 3.

```
<Sysname> system-view
[Sysname] vlan 3
[Sysname-vlan3] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port access vlan 3
```

port hybrid pvid vlan

Syntax **port hybrid pvid vlan** *vlan-id*

undo port hybrid pvid

View Ethernet interface view, port group view

Parameter *vlan-id* : VLAN ID, in the range 1 to 4094.

Description Use the **port hybrid pvid vlan** command to configure the default VLAN ID of the Hybrid port.

Use the **undo port hybrid pvid** command to restore the default, VLAN 1.

Execution of the **undo vlan** command on a Hybrid port to remove the default VLAN does not affect the default VLAN configuration. That is to say, the non-existent VLAN can still be the default VLAN.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

The default VLAN ID of local Hybrid port must be consistent with that of the peer; otherwise, packets cannot be forwarded properly.

Related command: **port link-type**.

Example # Configure the default VLAN ID for the Hybrid port Ethernet 1/0 to be 100.

```
<Sysname> system-view
[Sysname] vlan 100
[Sysname-vlan100] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type hybrid
[Sysname-Ethernet1/0] port hybrid pvid vlan 100
```

port hybrid vlan

Syntax **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** }

undo port hybrid vlan *vlan-id-list*

View Ethernet interface view, port group view

Parameter *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4,094 and &<1-10> indicates that you can specify up to 10 times.

tagged: Specifies to tag the packets of the specified VLAN (s).

untagged: Specifies not to tag the specified VLAN(s).

Description Use the **port hybrid vlan** command to add the current Hybrid port to the specified VLAN(s).

Use the **undo port hybrid vlan** command to remove the current Hybrid port from the specified VLAN(s).

A hybrid port can belong to multiple VLANs and thus can allow packets of multiple VLANs to pass. Repetitive execution of the **port hybrid vlan** *vlan-id-list* { **tagged** | **untagged** } command will yield a set VLANs, to which the Hybrid port belongs.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to “Link Aggregation Configuration Commands” on page 473 for information about port groups.

Related command: **port link-type**.

Example # Add the Hybrid port Ethernet 1/0 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100. Tag all packets of these VLANs.

```
<Sysname> system-view
[Sysname] vlan all
Please wait... Done.
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type hybrid
[Sysname-Ethernet1/0] port hybrid vlan 2 4 50 to 100 tagged
```

port link-type

Syntax **port link-type** { **access** | **hybrid** | **trunk** }

undo port link-type

View Ethernet interface view, port group view

Parameter **access**: Configures the link type of a port as Access.

hybrid: Configures the link type of a port as Hybrid.

trunk: Configures the link type of a port as Trunk.

Description Use the **port link-type** command to configure the link type of a port.

Use the **undo port link-type** command to restore the default link type of a port.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

By default, a port is an Access port.

Example # Configure Ethernet 1/0 to be a Trunk port.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type trunk
```

port trunk permit vlan

Syntax **port trunk permit vlan** { *vlan-id-list* | **all** }

undo port trunk permit vlan { *vlan-id-list* | **all** }

View Ethernet interface view, port group view

Parameter *vlan-id-list*: The range of VLANs that the Hybrid ports will be added to, in the format of *vlan-id-list* = [*vlan-id1* [**to** *vlan-id2*]]&<1-10>, where *vlan-id* ranges from 1 to 4,094 and &<1-10> indicates that you can specify up to 10 parameters.

all: Adds the Trunk port to all VLANs.

Description Use the **port trunk permit vlan** command to add a Trunk port to a specified VLAN, a selection of VLANs, or all VLANs.

Use the **undo port trunk permit vlan** command to remove the Trunk port from a specified VLAN, a selection of VLANs, or all VLANs.

The Trunk port can allow multiple VLANs to pass. Repetitive execution of the **port trunk permit vlan** command will yield a set of *vlan-id-list*, to which the Trunk port belongs.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

Related command: **port link-type**.

Example # Add the Trunk port Ethernet 1/0 to VLAN 2, VLAN 4, and the range of VLANs from VLAN 50 to VLAN 100.

```
<Sysname> system-view
[Sysname] vlan all
Please wait... Done.
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type trunk
[Sysname-Ethernet1/0] port trunk permit vlan 2 4 50 to 100
Please wait.......... Done.
```

port trunk pvid vlan

Syntax **port trunk pvid vlan** *vlan-id*

undo port trunk pvid

View Ethernet interface view, port group view

Parameter *vlan-id* : VLAN ID, in the range of 1 to 4,094

Description Use the **port trunk pvid vlan** command to configure the default VLAN ID for the Trunk port.

Use the **undo port trunk pvid** command to restore the default.

By default, the default VLAN on a Trunk port is VLAN 1.

Execution of the **undo vlan** command on a Trunk port to remove a default VLAN does not affect the default VLAN configurations. That is to say, a non-existent VLAN can still be the default VLAN.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

You must configure the same default VLAN ID for the Trunk port of both the local device and remote device. Otherwise, the packets cannot be transmitted correctly.

Related command: **port link-type**.

Example # Configure the default VLAN ID for the Trunk port Ethernet 1/0 as 100.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port link-type trunk
[Sysname-Ethernet1/0] port trunk pvid vlan 100
```

41 VOICE VLAN CONFIGURATION COMMANDS

- *Voice VLAN automatic mode and secure mode are not supported on MSR 20 series routers.*
- *Voice VLAN automatic mode and secure mode are not supported on SIC-4FSW and DSIC-9FSW modules.*
- *Voice VLAN automatic mode and secure mode are supported on 16FSW and 24FSW modules.*

display voice vlan oui

Syntax **display voice vlan oui**

View Any view

Parameter None

Description Use the **display voice vlan oui** command to display the Organizationally Unique Identifier (OUI) address(es), the OUI address mask, and the descriptive string currently supported by system.

Related command: **voice vlan**, **voice vlan enable**.

As the first 24 bits of a MAC address (in binary format), an OUI address is a globally unique identifier assigned to a vendor by IEEE.

Example # Display the OUI address of a voice VLAN.

```
<Sysname> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
```

Table 113 Description on the fields of the display voice vlan oui command

Field	Description
Oui Address	OUI addresses that are allowed to pass
Mask	Mask of the OUI addresses that are allowed to pass

Table 113 Description on the fields of the display voice vlan oui command

Field	Description
Description	Description of the OUI addresses that are allowed to pass

display voice vlan state

Syntax **display voice vlan state**

View Any view

Parameter None

Description Use the **display voice vlan state** command to display the voice VLAN configuration.

Related command: **voice vlan enable**.

Example # Display the voice VLAN configurations.

```
<Sysname> display voice vlan state
Voice VLAN status: ENABLE
Voice VLAN ID: 2
Voice VLAN security mode: Security
Voice VLAN aging time: 1440 minutes
Voice VLAN enabled port and its mode:
PORT               MODE
--------------------------------
Ethernet1/2        MANUAL
Ethernet1/3        MANUAL
Ethernet1/4        MANUAL
Ethernet1/5        AUTO
```

Table 114 Description on the fields of the display voice vlan state command

Field	Description
Voice VLAN status	The current voice VLAN status, that is, whether it is enabled or disabled.
Voice VLAN ID	ID of a voice VLAN
Voice VLAN security mode	Security mode of a voice VLAN
Voice VLAN aging time	Aging time of a voice VLAN
Current voice vlan enabled port and its mode	The port that is currently enabled with the voice VLAN feature and its working mode
PORT	port ID
MODE	Voice VLAN working mode: manual or automatic.

voice vlan

Syntax **voice vlan** *vlan-id* **enable**

undo voice vlan enable

View System view

Parameter *vlan-id*: ID of the VLAN to be enabled with the voice VLAN feature, in the range of 2 to 4,094.

Description Use the **voice vlan** command to enable the voice VLAN feature globally.

Use the **undo voice vlan enable** command to disable the voice VLAN feature globally.

- At one particular moment, only one VLAN of a certain device can have the voice VLAN feature enabled.
- Ensure that a VLAN exists before enabling its voice VLAN feature and that it is not VLAN 1. Otherwise, the configurations will fail.
- If a VLAN to be deleted has the voice VLAN feature enabled, you need to disable the voice VLAN feature first before deleting the VLAN.

Related command: **display voice vlan state**.

Example # Enable the voice VLAN feature on VLAN 2(assuming that VLAN 2 already exists).

```
<Sysname> system-view
[Sysname] voice vlan 2 enable
```

voice vlan aging

Syntax **voice vlan aging** *minutes*

undo voice vlan aging

View System view

Parameter *minutes*: Aging time of a voice VLAN, in the range 5 to 43,200 minutes. This value is 1,440 by default.

Description Use the **voice vlan aging** command to configure the aging time of a voice VLAN.

Use the **undo voice vlan aging** command to restore the aging time of a voice VLAN.

Under automatic mode, the system will decide whether to add a port to a voice VLAN based on the source MAC address contained in its inbound voice packets. After adding a port to the voice VLAN, the system will start the aging timer at the same time. If within the aging time, no voice packets is received from the port, it will be removed from the voice VLAN when the aging time expires.

Related command: **display voice vlan state**.

Example # Configure the aging time of the voice VLAN as 100 minutes.

```
<Sysname> system-view
[Sysname] voice vlan aging 100
```

voice vlan enable

Syntax **voice vlan enable**

undo voice vlan enable

View Ethernet interface view

Parameter None

Description Use the **voice vlan enable** command to enable the voice VLAN feature on an Ethernet port.

Use the **undo voice vlan enable** command to disable the voice VLAN feature on an Ethernet port.

No voice VLAN is enabled on a port by default.

- Under automatic mode, only The Trunk or Hybrid port can be configured with the voice VLAN feature. The Access port cannot be configured with this feature.
- Before enabling the voice VLAN feature on a port, ensure that its is enabled globally first
- Only after the voice VLAN feature is enabled under both system view and Ethernet interface view will it functions properly.

Example # Enable the voice VLAN attribute on the port Ethernet 1/0.

```
<Sysname> system-view
[Sysname] voice vlan 2 enable
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] voice vlan enable
```

voice vlan mac-address

Syntax **voice vlan mac-address** *mac-addr* **mask** *oui-mask* [**description** *text*]

undo voice vlan mac-address *oui*

View System view

Parameter *mac-addr*: MAC address, in the format of H-H-H, such as 1234-1234-1234.

mask *oui-mask*: Valid length of the OUI address, represented in mask, in the format of H-H-H, from left to right are consecutive fs and 0s, for example, ffff-f000-0000.

description *text*: A case sensitive string that describes the OUI address, in the range of 1 to 30 characters.

oui: Deletes an OUI address that is in the format H-H-H, such as 1234-1200-0000, which is the logic AND result of *mac-addr* and *oui-mask.* Using the **display voice vlan oui** command can display OUI address information. The OUI address cannot be a broadcast, multicast or address of all 0s or all fs.

Description Use the **voice vlan mac-address** command to make a specified OUI address identified by the voice VLAN.

Use the **undo voice vlan mac-address** command to remove an OUI address from being identified by the voice VLAN.

A maximum of 16 OUI addresses can be supported by the system.

The system default OUI addresses, which can be removed or then added, are illustrated in the following table.

Table 115 Default OUI addresses

Number	OUI	Description
1	0001-e300-0000	Siemens phone
2	0003-6b00-0000	Cisco phone
3	0004-0d00-0000	Avaya phone
4	00d0-1e00-0000	Pingtel phone
5	0060-b900-0000	Philips/NEC phone
6	00e0-7500-0000	Polycom phone
7	00e0-bb00-0000	3com phone

Related command: **display voice vlan oui**.

Example # Configure the OUI address as 1234-1234-1234, the mask as ffff-ff00-0000, and the descriptive string as phone A, that is, voice packets from Phone A with source MAC address being 1234-1234-1234 can pass through the voice VLAN.

```
<Sysname> system-view
[Sysname] voice vlan mac-address 1234-1234-1234 mask ffff-ff00-0000
description PhoneA
```

Display OUI address information.

```
<Sysname> display voice vlan oui
Oui Address     Mask            Description
0001-e300-0000  ffff-ff00-0000  Siemens phone
0003-6b00-0000  ffff-ff00-0000  Cisco phone
0004-0d00-0000  ffff-ff00-0000  Avaya phone
00d0-1e00-0000  ffff-ff00-0000  Pingtel phone
0060-b900-0000  ffff-ff00-0000  Philips/NEC phone
```

```
00e0-7500-0000  ffff-ff00-0000  Polycom phone
00e0-bb00-0000  ffff-ff00-0000  3com phone
1234-1200-0000  ffff-ff00-0000  PhoneA
```

Disable voice packets of Phone A from passing through the voice VLAN.

```
<Sysname> system-view
[Sysname] undo voice vlan mac-address 1234-1200-0000
```

voice vlan mode auto

Syntax **voice vlan mode auto**

undo voice vlan mode auto

View Ethernet interface view

Parameter None

Description Use the **voice vlan mode auto** command to configure the voice VLAN working mode on a port to be automatic.

Use the **undo voice vlan mode auto** command to configure the voice VLAN working mode on a port to be manual.

By default, the voice VLAN working mode is automatic.

The voice VLAN working mode of a port is independent of those of other ports.

Note that: if a port is enabled with voice VLAN in manual mode, you need to add the port to the voice VLAN manually to validate the voice VLAN.

Example # Configure the voice VLAN working mode on Ethernet 1/0 as manual.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo voice vlan mode auto
```

voice vlan security enable

Syntax **voice vlan security enable**

undo voice vlan security enable

View System view

Parameter None

Description Use the **voice vlan security enable** command to enable the security mode for voice VLAN.

Use the **undo voice vlan security enable** command to disable the security mode for voice VLAN.

By default, the security mode of voice VLAN is enabled.

*The **voice vlan security enable** and **undo voice vlan security enable** commands take effect only after the voice VLAN attribute is enabled globally.*

Example # Disable the security mode of the voice VLAN.

```
<Sysname> system-view
[Sysname] undo voice vlan security enable
```

42 PORT ISOLATION CONFIGURATION COMMANDS

display port-isolate group

Syntax **display port-isolate group**

View Any view

Parameter None

Description Use the **display port-isolate group** command to display information of the default isolation group (Group 1).

Example # Display information of the default isolation group.

```
<Sysname> display port-isolate group
 Port-isolate group information:
 Uplink port support: NO
 Group ID: 1
    Ethernet1/1                Ethernet1/2
```

Table 116 Description on the output information of the display port-isolate group command

Field	Description
Port-isolate group information	Information of the isolation group
Uplink port support	Whether support uplink port
Group ID	Isolation group number
Ethernet1/1 Ethernet1/2	Ordinary ports (non-uplink ports) in the isolation group

port-isolate enable

Syntax **port-isolate enable**

undo port-isolate enable

View Ethernet interface view, port group view

Parameter None

Description Use the **port-isolate enable** command to add the current port to the default isolation group (Group 1) as an ordinary port.

Use the **undo port-isolate enable** command to remove the port from the isolation group.

Configured in Ethernet interface view, the setting is effective on the current port only; configured in port group view, the setting is effective on all ports in the port group.

Refer to "Link Aggregation Configuration Commands" on page 473 for information about port groups.

This command adds a port to the default isolation group 1.

Example # Add port Ethernet 1/0 to isolation group 1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] port-isolate enable
```

43 DYNAMIC ROUTE BACKUP CONFIGURATION COMMANDS

Refer to "DCC Configuration Commands" on page 315 for more information about dial control center (DCC).

standby routing-group

Syntax **standby routing-group** *group-number*

undo standby routing-group *group-number*

View Interface view

Parameter *group-number*: Dynamic route backup group number, ranging from 1 to 255.

Description Use the **standby routing-group** command to enable the dynamic route backup function on a dialup interface.

Use the **undo standby routing-group** command to disable the dynamic route backup function.

By default, the dynamic route backup function is disabled.

Before enabling the dynamic route backup function on a dialup interface, make sure that DCC has been enabled on the dialup interface.

Example # Enable the dynamic route backup function on Bri 3/0.

```
<Sysname> system-view
[Sysname] interface bri 3/0
[Sysname-Bri3/0] standby routing-group 1
```

standby routing-rule

Syntax **standby routing-rule** *group-number* **ip** *ip-address* { *mask* | *mask-length* }

undo standby routing-rule *group-number* [**ip** *ip-address* { *mask* | *mask-length* }]

View System view

Parameter *group-number*: Dynamic route backup group number, ranging from 1 to 255.

ip *ip-address*: IP address of the network segment to be monitored.

mask: Network mask.

mask-length: Network mask length, ranging from 0 to 32.

Description Use the **standby routing-rule** command to create a dynamic route backup group and add the network segment to be monitored to this group.

Use the **undo standby routing-rule** command to remove a dynamic route backup group or remove the monitored network segment from this group.

By default, no dynamic route backup group is created.

Up to 255 monitored network segments can be added to a dynamic route backup group. The primary link is considered to be disconnected when there is no valid route to any of the monitored network segments in a dynamic route backup group.

Example # Create dynamic route backup group 1 to monitor routes to the network segments 20.0.0.0/8 and 30.0.0.0/8.

```
<Sysname> system-view
[Sysname] standby routing-rule 1 ip 20.0.0.1 255.0.0.0
[Sysname] standby routing-rule 1 ip 30.0.0.1 255.0.0.0
```

standby timer routing-disable

Syntax **standby timer routing-disable** *seconds*

undo standby timer routing-disable

View Interface view

Parameter *seconds*: Delay between primary link connection and backup link disconnection, ranging from 0 to 65,535 in seconds.

Description Use the **standby timer routing-disable** command to configure the delay between primary link connection and backup link disconnection. .

Use the **undo standby timer routing-disable** command to restore the default.

By default, the delay between primary link connection and backup link disconnection is 20 seconds.

Example # Set the delay between primary link connection and backup link disconnection to 5 seconds on Bri 3/0.

```
<Sysname> system-view
[Sysname] interface bri 3/0
[Sysname-Bri3/0] standby timer routing-disable 5
```

44 LOGICAL INTERFACE CONFIGURATION COMMANDS

This section introduces basic configurations about logical interfaces. For the configurations about the data link layer, the network layer and some special features, refer to the relevant sections in Chapter 1 through Chapter 37 and Chapter 46 through Chapter 70.

broadcast-limit link

Syntax **broadcast-limit link** *number*

undo broadcast-limit link

View Virtual template (VT) view

Parameter *number*: Maximum number of links that can send multicast or broadcast packets in a VT. This argument ranges from 0 to 128 and defaults to 30. The value 0 indicates that multicast packets or broadcast packets cannot be sent.

Description Use the **broadcast-limit link** command to set the maximum number of links that can send multicast or broadcast packets in a VT. Use the **undo broadcast-limit link** command to restore the default setting.

When a VT has plenty of links, the system performance will be decreased if all the links send multicast or broadcast packets. In this case, you can use the **broadcast-limit link** command to limit the maximum number of links that can send multicast packets or broadcast packets.

Example # Set the maximum number of links that can send multicast or broadcast packets in VT 1 to 100.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1] broadcast-limit link 100
```

display interface loopback

Syntax **display interface loopback** [*number*]

View Any view

Parameter *number*: Loopback interface number, which can be the number of any existing Loopback interface.

Description Use the **display interface loopback** command to view the relevant information about the existing Loopback interfaces. If you do not provide a Loopback interface number, this command will display the relevant information about all the existing Loopback interfaces.

Related command: **interface loopback**.

Example # View the status of Loopback 12.

```
<Sysname> display interface loopback 12
LoopBack12 current state: UP
Line protocol current state: UP (spoofing)
Description: LoopBack12 Interface
The Maximum Transmit Unit is 1536
Internet protocol processing : disabled
Physical is Loopback
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes, 0 drops
```

Table 117 Description on the fields of the display interface loopback command

Field	Description
current state	Physical state of the interface: UP/DOWN
Line protocol current state	State of the link layer protocol: UP/DOWN
Description	Description string of the interface
The Maximum Transmit Unit	Maximum transmit unit (MTU) of the interface
Internet protocol processing	Processing state of the network layer protocol: enabled/disabled
Physical	Physical type of the interface
Last 300 seconds input: 0 bytes/sec 0 packets/sec	Statistics on packets sent/received over the physical layer
Last 300 seconds output: 0 bytes/sec 0 packets/sec	
0 packets input, 0 bytes, 0 drops	
0 packets output, 0 bytes, 0 drops	

display interface mfr

Syntax **display interface mfr** [*mfr-number*]

View Any view

Parameter *mfr-number*: Multilink frame relay (MFR) interface number, which can be the number of any existing MFR interface.

Description Use the **display interface mfr** command to view the state information about the existing MFR interfaces. If you do not provide an MFR interface number, this command will display the state information about all the existing MFR interfaces.

Related command: **interface mfr**.

Example # View the state information about MFR 2.

```
<Sysname> display interface mfr 2
MFR2 current state: DOWN
Line protocol current state: DOWN
Description: MFR2 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is FR IETF
  LMI DLCI is 0, LMI type is Q.933a, frame relay DTE
  LMI status enquiry sent 0, LMI status received 0
  LMI status timeout 0, LMI message discarded 0
Physical is MFR
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes, 0 drops
```

Table 118 Description on the fields of the display interface mfr command

Field	Description
current state	Physical state of the interface: UP/DOWN
Line protocol current state	State of the link layer protocol: UP/DOWN
Description	Description string of the interface
The Maximum Transmit Unit	Maximum transmit unit (MTU) of the interface
Internet protocol processing	Processing state of the network layer protocol: enabled/disabled
Link layer protocol	Link layer protocol
LMI DLCI	Data link connection identifier (DLCI) used by the local management interface (LMI)
LMI type	Type of the LMI
frame relay	Type of the frame relay device
LMI status enquiry sent 0, LMI status received 0	Statistics on packets sent/received over the link layer
LMI status timeout 0, LMI message discarded 0	
Physical	Physical type of the interface

Table 118 Description on the fields of the display interface mfr command

Field	Description
Output queue : (Urgent queue : Size/Length/Discards)	Statistics on packets sent/received over the physical layer
Output queue : (Protocol queue : Size/Length/Discards)	
Output queue : (FIFO queuing : Size/Length/Discards)	
Last 300 seconds input: 0 bytes/sec, 0 packets/sec	
Last 300 seconds output: 0 bytes/sec, 0 packets/sec	
0 packets input, 0 bytes, 0 drops	
0 packets output, 0 bytes, 0 drops	

display interface mp-group

Syntax **display interface mp-group** [*mp-number*]

View Any view

Parameter *mp-number:* Multilink point to point protocol group (MP-group) interface number, which can be the number of any existing MP-group interface.

Description Use the **display interface mp-group** command to view the state information about the existing MP-group interfaces. If you do not provide an MP-group interface number, this command will display the state information about all the existing MP-group interfaces.

Related command: **interface mp-group**.

Example # View the state information of MP-group 12.

```
<Sysname> display interface mp-group 12
Mp-group12 current state: DOWN
Line protocol current state: DOWN
Description: Mp-group12 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is MP
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes, 0 drops
```

The "Hold timer" field of the **display interface mp-group** command represents the hold time of the link state (up/down) of the current interface, and the "LCP initial" field indicates that the link control protocol (LCP) is initialized. Refer to Table 117 for the description on the other fields.

display interface null

Syntax **display interface** null [**0**]

View Any view

Parameter **0**: Null interface number. This argument is always 0.

Description Use the **display interface null** command to view the state information about the null interface. Even if this argument is not specified, the state information about null interface 0 is displayed, because there is only one interface.

Related command: **interface null**.

Example # View the state information about null 0.

```
<Sysname> display interface null 0
NULL0 current state :UP
Line protocol current state :UP (spoofing)
Description :  NULL0 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
Physical is NULL DEV
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes, 0 drops
```

Refer to Table 117 for the description on the fields of the **display interface null** command.

display interface virtual-ethernet

Syntax **display interface virtual-ethernet** [*number*]

View Any view

Parameter *number*: Virtual Ethernet (VE) interface number, which can be the number of any existing VE interface.

Description Use the **display interface virtual-ethernet** command to view the state information about the existing VE interfaces. If you do not provide a VE interface number, this command will display the state information about all the existing VE interfaces.

Related command: **interface virtual-ethernet**.

Example # View the state information about VE 12.

```
<Sysname> display interface virtual-ethernet 12
Virtual-Ethernet2 current state: UP
Line protocol current state: UP
Description: Virtual-Ethernet2 Interface
The Maximum Transmit Unit is 1500
Internet protocol processing : disabled
IP Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e200-1234
IPv6 Packet Frame Type: PKTFMT_ETHNT_2,  Hardware Address: 000f-e200-1234
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards)  0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
```

Table 119 Description on the fields of the display interface virtual-ethernet command

Field	Description
current state	Physical state of the interface: UP/DOWN
Line protocol current state	State of the link layer protocol: UP/DOWN
Description	Description string of the interface
The Maximum Transmit Unit	MTU of the interface
Internet protocol processing	Processing state of the network layer protocol: enabled/disabled
IP Packet Frame Type	Encapsulation format of IP packets
Hardware Address	Hardware address (MAC addresses)
IPv6 Packet Frame Type	Encapsulation format of IPv6 packets
Output queue : (Urgent queue : Size/Length/Discards)	Statistics on output queues
Output queue : (Protocol queue : Size/Length/Discards)	
Output queue : (FIFO queuing : Size/Length/Discards)	

display interface virtual-template

Syntax **display interface virtual-template** [*number*]

View Any view

Parameter *number*: VT number, which can be the number of any existing VT.

Description Use the **display interface virtual-template** command to view the state information about the existing VTs. If you do not provide a VT number, this command will display the state information about all the existing VTs.

Related command: **interface virtual-template**.

Example # View the state information about VT 1.

```
<Sysname> display interface virtual-template 1
Virtual-Template1 current state: UP
```

```
Line protocol current state: UP (spoofing)
Description: Virtual-Template1 Interface
The Maximum Transmit Unit is 1500, Hold timer is 10(sec)
Internet protocol processing : disabled
Link layer protocol is PPP
LCP initial
Physical is None
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
    0 packets input, 0 bytes, 0 drops
0 packets output, 0 bytes, 0 drops
```

The "LCP initial" field of the **display interface virtual-template** command indicates that LCP is initialized. Refer to Table 117 for the description on the other fields.

display mfr

Syntax **display mfr** [**interface** *interface-type interface-number* | **verbose**]

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

verbose: Displays the detailed statistics.

Description Use the **display mfr** command to display the configuration information and statistics information about the MFR bundle and bundled links.

Example # Display the configuration information and state information about all the MFR bundles and bundled links.

```
<Sysname> display mfr
Bundle interface:MFR0, Bundle State = up, Bundle Class = A
    fragment disabled
    Bundle name = MFR0
    Bundle links:
Serial1/0, PHY state = up, link state = up, Link name = Serial1/0
```

Table 120 Description of the fields of the display mfr command

Field	Description
Bundle interface	Bundled interface
Bundle state	State of the bundled interface
Bundle class	If the bundle class is A, the state of the bundled interface is up only if one of the bundled links is up; when all the bundled links are down, the state of the bundled interface is shown as down.
fragment disabled	Whether fragmentation is enabled (in this example, fragmentation is disabled)

Table 120 Description of the fields of the display mfr command

Field	Description
Bundle name = MFR0	Name of the MFR bundling
Bundle links	Physical interface information on each bundled link
Serial1/0, PHY state = up, link state = up, Link name = Serial1/0	Physical interface of the bundled link, physical state of the interface, state of the link layer, and the name of the bundled link (name of the corresponding interface by default)

display virtual-access

Syntax **display virtual-access** [**dialer** *dialer-number* | **vt** *vt-number* | **user** *user-name* | **peer** *peer-address* | *va-number*]*

View Any view

Parameter *dialer-number*: Dialer interface number, ranging from 0 to 1023.

vt-number: Number of the VT where the virtual access (VA) interface resides. This argument ranges from 0 to 1023.

user-name: Name of the user accessing through the VA interface. This argument is a string of 1 character to 80 characters.

peer-address: Peer IP address of the VA interface, in dotted decimal notation.

va-number: Sequence number of the VA interface, ranging from 0 to 128.

Description Use the **display virtual-access** command to view the state information about the VA interfaces.

When necessary, the system will automatically create VA interfaces, which will adopt the parameters defined in a specific VT. You need not create and configure VA interfaces manually. VA interfaces will be removed due to underlying layer disconnection or user intervention.

Example # View the state information about all the VA interfaces.

```
<Sysname> display virtual-access vt 1
Virtual-Template1:0 current state :UP
Line protocol current state :UP
Description : Virtual-Template1:0 Interface
The Maximum Transmit Unit is 1500
Link layer protocol is PPP
LCP opened, MP opened, IPCP opened, OSICP opened
Physical is MP, baudrate: 64000
Output queue : (Urgent queue : Size/Length/Discards)  0/50/0
Output queue : (Protocol queue : Size/Length/Discards) 0/500/0
Output queue : (FIFO queuing : Size/Length/Discards)  0/75/0
    Last 300 seconds input:  0 bytes/sec 0 packets/sec
    Last 300 seconds output:  0 bytes/sec 0 packets/sec
```

```
    4 packets input, 50 bytes, 0 drops
4 packets output, 50 bytes, 0 drops
```

Refer to Table 117 for the description on the fields of the **display interface virtual-access** command.

interface

Syntax **interface** *interface-type interface-number.subnumber* [**p2mp** | **p2p**]

undo interface *interface-type interface-number.subnumber*

View System view

Parameter *interface-type interface-number.subnumber*: Interface type and interface number. The *interface-number* argument is the primary interface number, and the *subnumber* argument is the sub-interface number, ranging from 0 to 1023.

p2mp: Configures the type of a WAN sub-interface to be point-to-multipoint.

p2p: Configures the type of a WAN sub-interface to be point-to-point.

Description Use the **interface** *interface-type interface-number.subnumber* [**p2mp** | **p2p**] command to create a WAN sub-interface and enter WAN sub-interface view.

Use the **undo interface** command to remove the specified sub-interface.

Currently, point-to-multipoint or point-to-point sub-interfaces can be configured for ATM interfaces, frame relay interfaces or X.25 interfaces. By default, point-to-multipoint sub-interfaces are created.

A Layer 3 Ethernet interface can accommodate 1 to 4,096 sub-interfaces.

Example # Create a sub-interface on ATM 2/0.

```
<Sysname> system-view
[Sysname] interface atm 2/0.1
[Sysname-Atm2/0.1]
```

interface ethernet

Syntax **interface ethernet** *interface-number.subnumber*

undo interface ethernet *interface-number.subnumber*

View System view

Parameter *interface-number.subnumber*: Interface number. The *interface-number* argument is the primary interface number, and the *subnumber* argument is the sub-interface number, ranging from 1 to 4094.

Description Use the **interface ethernet** command to create an Ethernet sub-interface and enter the corresponding Ethernet sub-interface view.

Use the **undo interface ethernet** command to remove the specified Ethernet sub-interface.

By default, no VLAN is associated to an Ethernet sub-interface.

Note that the VLAN associated with the Ethernet sub-interface of the local device must be the same as the VLAN associated to the Ethernet sub-interface of the peer device. Otherwise, packets cannot be transmitted properly. A Layer 3 Ethernet interface can accommodate 1 to 4,096 sub-interfaces.

Example # Create a sub-interface on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0.1
[Sysname-Ethernet1/0.1]
```

interface loopback

Syntax **interface loopback** *number*

undo interface loopback *number*

View System view

Parameter *number*: Loopback interface number, ranging from 0 to 1023.

Description Use the **interface loopback** command to create a Loopback interface and enter the corresponding Loopback interface view.

Use the **undo interface loopback** command to remove the specified Loopback interface.

Related command: **display interface loopback**.

Example # Create Loopback 5.

```
<Sysname> system-view
[Sysname] interface loopback 5
[Sysname-LoopBack5]
```

interface mfr

Syntax **interface mfr** { *interface-number* | *interface-number.subnumber* }

undo interface mfr { *interface-number* | *interface-number.subnumber* }

View System view

Parameter *interface-number.subnumber*: Interface number. The *interface-number* argument is the primary interface number, and the *subnumber* argument is the sub-interface number, ranging from 0 to 1023.

Description Use the **interface mfr** command to create an MFR interface or an MFR sub-interface and enter the specified MFR interface view or MFR sub-interface view.

Use the **undo interface mfr** command to remove an MFR interface.

Create the corresponding MFR interface before creating an MFR sub-interface.

Example # Create MFR 3.

```
<Sysname> system-view
[Sysname] interface mfr 3
[Sysname-MFR3]
```

interface mp-group

Syntax **interface mp-group** *mp-number*

undo interface mp-group *mp-number*

View System view

Parameter *mp-number*: MP-group interface number, ranging from 0 to 1023.

Description Use the **interface mp-group** command to create an MP-group interface and enter the specified MP-group interface view.

Use the **undo interface mp-group** command to remove an MP-group interface.

This command can be used in conjunction with the **ppp mp mp-group** command. You can execute the two commands regardless of sequence.

Example # Create MP-group 3.

```
<Sysname> system-view
[Sysname] interface mp-group 3
[Sysname-Mp-group3]
```

interface null

Syntax **interface null 0**

View System view

Parameter **0**: Specifies the null interface number.

Description Use the **interface null** command to enter null interface view.

Only one null interface (Null 0) exists. Null 0 is always up, and cannot be brought down or removed.

Related command: **display interface null**.

Example # Enter Null 0 interface view.

```
<Sysname> system-view
[Sysname] interface null 0
[Sysname-NULL0]
```

interface virtual-ethernet

Syntax **interface virtual-ethernet** *number*

undo interface virtual-ethernet *number*

View System view

Parameter *number*: VE interface number, ranging from 0 to 1023.

Description Use the **interface virtual-ethernet** command to create a VE interface and enter the specified VE interface view.

Use the **undo interface virtual-ethernet** command to remove the specified VE interface.

Example # Create VE interface 12.

```
<Sysname> system-view
[Sysname] interface virtual-ethernet 12
[Sysname-Virtual-Ethernet12]
```

interface virtual-template

Syntax **interface virtual-template** *number*

undo interface virtual-template *number*

View System view

Parameter *number*: VT number, ranging from 0 to 1023.

Description Use the **interface virtual-template** command to create a VT and enter the specified VT view.

Use the **undo interface virtual-template** command to remove the specified VT.

Before removing a VT, make sure that all the relevant VA interfaces are removed and this virtual interface is not being used.

Example # Create VT 10.

```
<Sysname> system-view
[Sysname] interface virtual-template 10
[Sysname-Virtual-Template10]
```

45 CPOS INTERFACE CONFIGURATION COMMANDS

E1- and T1-related commands are available for the CPOS (E) interface modules only.

clock

Syntax **clock** { **master** | **slave** }

undo clock

View CPOS interface view

Parameter **master**: Sets the clock mode of the CPOS interface to master.

slave: Sets the clock mode of the CPOS interface to slave.

Description Use the **clock** command to set the clock mode of the CPOS interface.

Use the **undo clock** command to restore the default, that is, slave.

When connected to a SONET/SDH device, the CPOS interface must use the slave clock because the SONET/SDH network clock is more precise. When the interface is directly connected to another CPOS interface with fiber-optic, you only need to configure them with different clock modes.

Example # Set the clock mode of interface CPOS 1/0 to master.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] clock master
```

controller cpos

Syntax **controller cpos** *cpos-number*

View System view

Parameter *cpos-number*: CPOS interface number.

Description Use the **controller cpos** command to enter CPOS interface view.

Before you can configure a CPOS physical interface, you must enter its CPOS interface view.

Example # Enter the interface view of CPOS 1/0.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0]
```

---

crc

Syntax **crc** { **16** | **32** | **none** }

undo crc

View Synchronizing serial interface view

Parameter **16**: Sets the length of the CRC word to 16 bits.

32: Sets the length of the CRC word to 32 bits.

None: Disables CRC.

Description Use the **crc** command to set the CRC word length for a synchronizing serial interface formed by CPOS interfaces.

Use the **undo crc** command to restore the default.

The CRC word length for a synchronizing serial interface formed by CPOS interfaces defaults to 16 bits.

Example # Set the CRC word length to 16 bits for CPOS interface 1/0.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 3 channel-set 1 timeslot-list 1-31
[Sysname-Cpos1/0] quit
[Sysname] interface serial 1/0/3:1
[Sysname-Serial1/0/3:1] crc 16
```

---

display controller cpos

Syntax **display controller cpos** [*cpos-number*]

View Any view

Parameter *cpos-number*: CPOS interface number. If no CPOS number is specified, the information about all CPOS interfaces is displayed.

Description Use the **display controller cpos** command to display information about CPOS interfaces, such as state of E1/T1 channels, and alarms, and errors occurred to the regeneration section, multiplex section, and higher-order path.

The following table lists possible error types in the displayed information:

Table 121 Possible error types

Field	Description
FRED	Receive loss of basic frame alignment, or receive frames with red alarm errors.
COFA	Change of frame alignment.
SEF	Severely error frame. Four consecutive frame synchronization errors generate one SEF.
FERR	Framing Bit Error. It refers to the frame with the Ft/FPS/FAS error.
CERR	CRC error
FEBE	Far end block error. This occurs when the CRC4 framing format applies on the E1 channel.
BERR	PRBS bit error (Pseudo-random binary sequence bit error, for test only).
BIP	Bit-interleaved parity.
REI	Remote error indication.

In this table, FRED, COFA, and SEF are alarm errors (AERRs).

Related command: **display controller cpos e1**, **display controller cpos t1**.

Example # Display the path information of interface CPOS 4/0.

```
<Sysname> display controller cpos 4/0
Cpos4/0 current state : UP
Description : Cpos4/0 Interface
  Frame-format SDH, multiplex AU-3, clock master, loopback not set
  Tx: J0: 0x01, J1: "NetEngine", C2: 0x02
  Rx: J0: 0x01, J1: "NetEngine", C2: 0x02
Regenerator section:
  Alarm: none
  Error: 0 BIP, 0 SEF
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path(VC-3-1):
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path(VC-3-2):
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path(VC-3-3):
  Alarm: none
  Error: 0 BIP, 0 REI
Cpos4/0  CT1 1  is up
  Frame-format ESF, clock master, loopback not set
Cpos4/0  CT1 2  is up
  Frame-format ESF, clock master, loopback not set
```

```
Cpos4/0  CT1 3  is up
  Frame-format ESF, clock master, loopback not set
```

(Some information about T1 channels is omitted.)

```
Cpos4/0  CT1 83  is up
  Frame-format ESF, clock master, loopback not set
Cpos4/0  CT1 84  is up
  Frame-format ESF, clock master, loopback not set
```

Table 122 Description on the fields of the display controller cpos command

Field	Description
Cpos4/0 current state	Current physical state of the CPOS interface.
Description	Interface description.
Frame-format SDH, multiplex AU-3, clock master, loopback not set	Physical layer information of the CPOS interface: the framing format is set to SDH, AU-3 path is adopted, master clock (internal clock signal) is used, and loopback is disabled.
Tx: J0: 0x01, J1: "NetEngine", C2: 0x02	The sent overhead bytes.
Rx: J0: 0x01, J1: "NetEngine", C2: 0x02	The received overhead bytes.
Regenerator section:	Alarm and error statistics about the regeneration section.
Multiplex section:	Alarm and error statistics about the multiplex section.
Higher order path(VC-3-x):	Alarm and error statistics about the higher-order path. The x in "VC-3-x" indicates the path number. When adopting AU-3 path, one STM-1 has three higher-order paths because it is multiplexed by three VC-3s. In the AU-4 path, there is one higher-order path VC-4.
Alarm:	Alarm statistics.
Error:	Error statistics.
Cpos4/0 CT1 1 is up	The current physical state of T1 channel 1 of the CPOS interface 4/0.
Frame-format ESF, clock master, loopback not set	Physical layer information of T1 channels: the framing format is set to ESF, master clock (internal clock signal) is used, and loopback is disabled.

display controller cpos e1

Syntax **display controller cpos** *cpos-number* **e1** *e1-number*

View Any view

Parameter *cpos-number*: CPOS interface number.

e1-number: Number of an E1 channel on a CPOS interface, in the range 1 to 63.

Description Use the **display controller cpos e1** command to display the physical layer configuration information of the specified E1 channel on the specified CPOS interface.

Different from the **display controller cpos** command, this command can display the error and alarm information of lower-order paths and E1 frames.

Example # Display the status information of E1 channel 1 on interface CPOS 1/0.

```
<Sysname> display controller cpos 1/0 e1 1
Cpos1/0 current state : UP
Description : Cpos1/0 Interface
  Frame-format SDH, multiplex AU-4, clock master, loopback not set
  Tx: J0: 0x01, J1: "NetEngine", C2: 0x02
  Rx: J0: 0x01, J1: "NetEngine", C2: 0x02

Regenerator section:
  Alarm: none
  Error: 0 BIP, 0 SEF

Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI

Higher order path(VC-4-1):
  Alarm: none
  Error: 0 BIP, 0 REI

Lower order path:
  Alarm: none
  Error: 0 BIP, 0 REI

Cpos2/0  CE1 1 is up
  Frame-format NO-CRC4, clock slave, loopback not set

E1 framer(1-1-1-1):
  Alarm: none
  Error: 0 FERR, 0 FEBE, 0 AERR
```

In the output, "E1 framer(1-1-1-1)" presents how the E1 channel is multiplexed. 1-1-1-1 represents in order VC-4 number, TUG-3 number, TUG-2 number, and TUG-12 number for an E1 channel.

display controller cpos t1

Syntax **display controller cpos** *cpos-number* **t1** *t1-number*

View Any view

Parameter *cpos-number*: CPOS interface number.

t1-number: Number of a T1 channel on a CPOS interface, in the range 1 to 84.

Description Use the **display controller cpos t1** command to display the physical layer configuration information of a T1 channel on a CPOS interface.

Different from the **display controller cpos** command, this command can display the error and alarm information of lower-order paths and T1 frames.

Example # Display the status information of T1 channel 2 on interface CPOS 4/0.

```
<Sysname> display controller cpos 4/0 t1 2
Cpos4/0 current state : UP   Frame-format SDH, multiplex AU-3, clock
 master, loopback not set
  Tx: J0: 0x01, J1: "NetEngine", C2: 0x02
  Rx: J0: 0x01, J1: "NetEngine", C2: 0x02
Regenerator section:
  Alarm: none
  Error: 0 BIP, 0 SEF
Multiplex section:
  Alarm: none
  Error: 0 BIP, 0 REI
Higher order path(VC-3-2):
  Alarm: none
  Error: 0 BIP, 0 REI
Lower order path:
  Alarm: none
  Error: 4095 BIP, 2047 REI
Cpos4/0  CT1 2 is up
  Frame-format ESF, clock master, loopback not set
T1 framer(2-1-1):
  Alarm: none
  Error: 4095 FERR, 79 AERR
```

Table 123 Description on the fields of the display controller cpos t1 command

Field	Description
Cpos4/0 current state	The current physical state of the CPOS interface
Frame-format SDH, multiplex AU-3, clock master, loopback not set	Physical layer information of the CPOS interface: the framing format is set to SDH, AU-3 path is adopted, master clock (internal clock signal) is used, and loopback is disabled.
Tx: J0: 0x01, J1: “NetEngine”, C2: 0x02	The sent overhead bytes.
Rx: J0: 0x01, J1: “NetEngine”, C2: 0x02	The received overhead bytes.
Regenerator section	Alarms and errors about the regeneration section.
Multiplex section	Alarms and errors about the regeneration section.
Higher order path(VC-3-2)	Alarm and error statistics about the higher-order path to which the T1 channel belongs. VC-3-2 means the second VC-3.
Lower order path	Alarm and error statistics about the lower-order path.
Error	Error statistics.
Cpos4/0 CT1 2 is up	The current physical state of T1 channel 2 on interface CPOS 4/0.
Frame-format ESF, clock master, loopback not set	Information about the physical layer of the T1 channel: the framing format is set to ESF, master clock (internal clock signal) is used, loopback is disabled.

Table 123 Description on the fields of the display controller cpos t1 command

Field	Description
T1 framer(2-1-1):	Presents how the T1 channel is multiplexed. 2-1-1 represents in order VC-3 number, TUG-2 number, and TUG-11 number for the T1 channel. For its calculation principle, refer to the accompanied operation manual.

e1 channel-set

Syntax **e1** *e1-number* **channel-set** *set-number* **timeslot-list** *range*

undo e1 *e1-number* **channel-set** *set-number*

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

set-number: Channel set number, in the range 0 to 30.

timeslot-list *range*: Specifies a list of timeslots assigned to the channel set. The *range* argument is in the range 1 to 31. While specifying timeslots, you can specify a single timeslot in the form of a *number*, or timeslots in a range in the form of *number1-number2*, or multiple timeslots in the form of *number1, number2-number3*.

Description Use the **e1 channel-set** command to bundle multiple timeslots on an E1 channel into one channel set.

Use the **undo e1 channel-set** command to remove the channel set (also mentioned as a bundle throughout this document).

By default, timeslot bundling is disabled on E1 channels.

When the E1 channel is channelized, its timeslot 0 is used for synchronization and the other 31 timeslots can be bundled to form one or multiple serial interfaces. These serial interfaces are numbered in the form of *interface number***/***channel number***:***channel set number*.

To guarantee the processing capacity of the system, you can have only up to 256 virtual serial interfaces on one CPOS physical interface.

Related command: **e1 unframed**.

Example # Bundle timeslots on E1 channel 63.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 63 channel-set 1 timeslot-list 1-31
```

Enter the view of the serial interface formed by the timeslot bundle.

```
[Sysname-Cpos1/0] quit
[Sysname] interface serial 1/0/63:1
[Sysname-Serial1/0/63:1]
```

e1 set clock

Syntax **e1** *e1-number* **set clock** { **master** | **slave** }

undo e1 *e1-number* **set clock**

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

master: Sets the clock mode of the E1 channel to master.

slave: Sets the clock mode of the E1 channel to slave.

Description Use the **e1 set clock** command to set the clock mode of the E1 channel.

Use the **undo e1 set clock** command to restore the default, that is, slave.

E1 channels on the same CPOS physical interface can use different clock modes, depending on connected devices. For example, when connected to a SONET/SDH device, an E1 channel should use the slave clock mode, and when directly connected to another device with fiber-optic, it can use either mode so long as the mode is different from the one used at the opposite end.

Note that different E1 channels of the same CPOS physical interface are independent of one another in terms of clock mode.

Example # Set the clock mode of E1 channel 1 to master.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 1 set clock master
```

e1 set frame-format

Syntax **e1** *e1-number* **set frame-format** { **crc4** | **no-crc4** }

undo e1 *e1-number* **set frame-format**

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

crc4: Sets the framing format to CRC4.

no-crc4: Sets the framing format to no-CRC4.

Description Use the **e1 set frame-format** command to set the framing format of an E1 channel.

Use the **undo e1 set frame-format** command to restore the default, that is, no-CRC4.

Example # Set E1 channel 1 to use framing format CRC4.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 1 set frame-format crc4
```

e1 set loopback

Syntax **e1** *e1-number* **set loopback** { **local** | **payload** | **remote** }

undo e1 *e1-number* **set loopback**

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

local: Enables internal loopback on the E1 channel.

payload: Enables external payload loopback on the E1 channel.

remote: Enables external loopback on the E1 channel.

Description Use the **e1 set loopback** command to configure the loopback mode of the E1 channel.

Use the **undo e1 set loopback** command to remove a loopback.

By default, loopback is disabled.

You may test E1 channels in different depths by using the **loopback** command with different keywords.

In an internal loopback, data of the sender is directly looped to the receiver.

In an external payload loopback, data received by the receiver is looped back at the E1 framer as payload.

In an external loopback, data received by the receiver is looped back directly without passing through the E1 framer.

Related command: **display controller cpos e1**.

Example # Enable external payload loopback on E1 channel 1.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 1 set loopback payload
```

e1 shutdown

Syntax **e1** *e1-number* **shutdown**

undo e1 *e1-number* **shutdown**

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

Description Use the **e1 shutdown** command to shut down an E1 channel.

Use the **undo e1 shutdown** command to bring up an E1 channel.

By default, E1 channels are enabled.

Disabling an E1 channel also disables the serial interfaces that are formed on it, if there is any.

Example # Shut down E1 channel 1.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] e1 1 shutdown
```

e1 unframed

Syntax **e1** *e1-number* **unframed**

undo e1 *e1-number* **unframed**

View CPOS interface view

Parameter *e1-number*: Number of an E1 channel on the CPOS interface, in the range 1 to 63.

Description Use the **e1 unframed** command to set an E1 channel on the CPOS interface to operate in unframed mode, that is, E1 mode.

Use the **undo e1 unframed** command to restore the default, that is, channelized mode.

So far, E1 channels on CPOS interfaces support two operating modes: clear channel (or unframed) and channelized.

- In unframed mode, an E1 channel can form a 2.048 Mbps serial interface without timeslot division. It is named **serial** *slot/port/e1-number***:0**.
- In channelized mode, all timeslots except timeslot 0 on the E1 channel can be bundled arbitrarily to form serial interfaces. Considering the system processing

capability, only up to 256 serial interfaces are allowed on one CPOS physical interface.

Example # Set E1 channel 3 on interface CPOS 1/0 to operate in unframed mode.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos 1/0] e1 3 unframed
```

flag

Syntax **flag** { **j0** *j0-string* | **j1** *j1-string* | **c2** *c2-value* }

undo flag { **j0** | **j1** | **c2** }

View CPOS interface view

Parameter **j0** *j0-string*: Specifies the regeneration section trace message. The *j0-string* argument is a string of 1 to 15 characters. The system default is 0x01.

j1 *j1-string*: Specifies the path trace message. The *j1-string* argument is a string of 1 to 15 characters. The system default is NetEngine.

c2 *c2-value*: Specifies the path signal label byte. The *c2-value* argument is a hexadecimal number in the range 0 to FF. The system default is 0x02.

Description Use the **flag** command to set the overhead byte of SONET/SDH frames.

Use the **undo flag** command to restore the default.

SONET/SDH frames provide a variety of overhead bytes for operation and maintenance (OAM) such as layered management on transmission networks. j1, j0 and c2 are used to support interoperability between devices in different countries and areas or from different vendors.

Related command: **display controller cpos**.

Example # Set J1 to aa on interface CPOS 1/0.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] flag j1 aa
```

frame-format

Syntax **frame-format** { **sdh** | **sonet** }

undo frame-format

View CPOS interface view

Parameter **sdh**: Sets framing format to synchronous digital hierarchy (SDH).

sonet: Sets framing format to synchronous optical network (SONET).

Description Use the **frame-format** command to configure framing on the CPOS interface.

Use the **undo frame-format** command to restore the default, that is, SDH.

Example # Set the framing format on interface CPOS 1/0 to SONET.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] frame-format sonet
```

loopback

Syntax **loopback** { **local** | **remote** }

undo loopback

View CPOS interface view

Parameter **local**: Internal loopback, used for testing the physical interface itself.

remote: External loopback, used for testing the cable connected to the interface.

Description Use the **loopback** command to configure the loopback mode on the CPOS interface.

Use the **undo loopback** command to remove a loopback.

By default, loopback is disabled.

Loopback is intended for test use. Disable it otherwise.

Example # Enable external loopback on interface CPOS 1/0.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] loopback remote
```

multiplex mode

Syntax **multiplex mode** { **au-3** | **au-4** }

undo multiplex mode

View CPOS interface view

Parameter **au-3**: Gets AUG through AU-3.

au-4: Gets AUG through AU-4.

Description Use the **multiplex mode** command to set AUG multiplexing mode.

Use the **undo multiplex mode** command to restore the default, that is, **au-4**.

SDH provides two payload mapping/multiplexing solutions: ANSI and ETSI.

- ANSI uses the AU-3 multiplexing scheme, where the lower-order payload is aggregated into the VC-3 higher-order path. VC-3 plus an AU pointer forms AU-3. Three such AU-3s can be synchronized and multiplexed to form one AUG.
- ETSI uses the AU-4 multiplexing scheme, where the lower-order payload is aggregated into the VC-4 higher-order path. VC-4 plus an AU pointer forms an AU-4. This AU-4 can be synchronized and multiplexed to form one AUG.

When the CPOS interface is operating in SDH mode, you can choose to multiplex AUG to AU-4 or AU-3 by using the **multiplex mode** command. When the CPOS interface is operating in SONET mode, AUG can be multiplexed only to AU-3 and the **multiplex mode** command is invalid in this case.

Related command: **frame-format**.

Example # In SDH mode, multiplex AUG to AU-3.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] frame-format sdh
[Sysname-Cpos1/0] multiplex mode au-
```

shutdown

Syntax **shutdown**

undo shutdown

View CPOS interface view

Parameter None

Description Use the **shutdown** command to shut down the CPOS physical interface.

Use the **undo shutdown** command to bring up the CPOS physical interface.

By default, the CPOS physical interface is up.

The **shutdown** command on the CPOS physical interface shuts down all E1/T1 channels and serial interfaces formed by timeslot bundles. They stop transmitting and receiving data as a result. To bring up them, perform the **undo shutdown** command on the CPOS physical interface.

Example # Shut down CPOS physical interface 1/0.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] shutdown
```

t1 channel-set

Syntax **t1** *t1-number* **channel-set** *set-number* **timeslot-list** *range* [**speed** { **56k** | **64k** }]

undo t1 *t1-number* **channel-set** *set-number*

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS interface, in the range 1 to 84.

set-number: Channel set number in the range 0 to 23.

timeslot-list *range*: Specifies a list of timeslots assigned to the channel set. The *range* argument is in the range of 1 to 24. While specifying timeslots, you can specify a single timeslot in the form of a *number*, or timeslots in a range in the form of *number1-number2*, or multiple timeslots in the form of *number1, number2-number3*.

speed { **56k** | **64k** }: Specifies how timeslots are bundled. If the **56k** keyword applies, timeslots form an N × 56 kbps bundle. If **64k** applies, timeslots form an N × 64 kbps bundle. If the speed is not specified, the default 64 kbps applies.

Description Use the **t1 channel-set** command to bundle timeslots on the T1 channel.

Use the **undo t1 channel-set** command to remove the bundle.

By default, timeslot bundling is disabled on T1 channels.

The serial interface formed by a timeslot bundle is numbered in the form of *interface number*/*channel number*:*channel set number*.

Related command: **t1 unframed**.

Example # Bundle timeslots on T1 channel 1.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] t1 1 channel-set 1 timeslot-list 1-23
```

Enter the serial interface view after the bundling operation.

```
[Sysname-Cpos1/0] quit
[Sysname] interface serial 1/0/1:1
[Sysname-Serial1/0/1:1]
```

t1 set clock

Syntax **t1** *t1-number* **set clock** { **master** | **slave** }

undo t1 *t1-number* **set clock**

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS, in the range 1 to 84.

Master: Set the clock mode of the T1 channel to master.

slave: Set the clock mode of the T1 channel to slave.

Description Use the **t1 set clock** command to configure the clock mode of the T1 channel.

Use the **undo t1 set clock** command to restore the default, that is, slave.

T1 channels on the same CPOS physical interface can use different clock modes, depending on connected devices. For example, when connected to a SONET/SDH device, a T1 channel should use the slave clock mode, and when directly connected to another device with fiber-optic, it can use either mode so long as the mode is different from the one used at the opposite end.

Note that different T1 channels of the same CPOS physical interface are independent of one another in terms of clock mode.

Example # Set the clock mode of T1 channel 1 to master.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] t1 1 set clock master
```

t1 set frame-format

Syntax **t1** *t1-number* **set frame-format** { **esf** | **sf** }

undo t1 *t1-number* **set frame-format**

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS interface, in the range 1 to 84.

esf: Sets the T1 channel to use the extended super frame (ESF) format.

sf: Sets the T1 channel to use the super frame (SF) format.

Description Use the **t1 set frame-format** command to set the framing format for T1 channel.

Use the **undo t1 set frame-format** command to restore the default, that is, ESF.

Example # Set the framing format of T1 channel 1 to SF.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] t1 1 set frame-format sf
```

t1 set loopback

Syntax **t1** *t1-number* **set loopback** { **local** | **payload** | **remote** }

undo t1 *t1-number* **set loopback**

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS interface, in the range 1 to 84.

local: Enables internal loopback.

payload: Enables external payload loopback.

remote: Enables external loopback.

Description Use the **t1 set loopback** command to configure the loopback mode of the T1 channel.

Use the **undo t1 set loopback** command to remove a loopback.

By default, loopback is disabled.

Loopback is intended for test use. Disable it otherwise.

Related command: **display controller cpos t1**.

Example # Enable external loopback on T1 channel 1.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] t1 1 set loopback payload
```

t1 shutdown

Syntax **t1** *t1-number* **shutdown**

undo t1 *t1-number* **shutdown**

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS interface, in the range 1 to 84.

Description Use the **t1 shutdown** command to shut down a T1 channel.

Use the **undo t1 shutdown** command to bring up a T1 channel.

By default, T1 channels are enabled.

Disabling a T1 channel disables the serial interfaces formed on it, if there is any.

Example # Shut down T1 channel 1.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos1/0] t1 1 shutdown
```

t1 unframed

Syntax **t1** *t1-number* **unframed**

undo t1 *t1-number* **unframed**

View CPOS interface view

Parameter *t1-number*: Number of a T1 channel on the CPOS interface, in the range 1 to 84.

Description Use the **t1 unframed** command to set a T1 channel on the CPOS interface to operate in unframed mode.

Use the **undo t1 unframed** command to restore the default, that is, channelized mode.

Like E1 channels, T1 channels on CPOS interfaces support unframed (clear channel) mode and channelized mode.

- In unframed mode, a T1 channel can form a 1.544 Mbps serial interface without timeslot division. This interface is named **serial** *slot/card/t1-number*:0.
- In channelized mode, 24 timeslots of T1 channel can be bound and used as serial interfaces.

Example # Set T1 channel 3 on interface CPOS 1/0 to operate in unframed mode.

```
<Sysname> system-view
[Sysname] controller cpos 1/0
[Sysname-Cpos 1/0] t1 3 unframed
```

46 ARP CONFIGURATION COMMANDS

arp check enable

Syntax **arp check enable**

undo arp check enable

View System view

Parameter None

Description Use the **arp check enable** command to enable ARP entry check, preventing the device from learning multicast MAC addresses. With this function enabled, the device cannot learn any ARP entry with a multicast MAC address. Configuring such a static ARP entry is not allowed either; otherwise, the system prompts error information.

Use the **undo arp check enable** command to disable the function, allowing the device to learn multicast MAC addresses. After the ARP entry check is disabled, the device can learn the ARP entry with a multicast MAC address, and you can also configure such a static ARP entry on the device.

By default, ARP entry check is enabled.

Example # Enable ARP entry check.

```
<Sysname> system-view
[Sysname] arp check enable
```

arp max-learning-num

Syntax **arp max-learning-num** *number*

undo arp max-learning-num

View VLAN interface view

Parameter *number*: Maximum number of dynamic ARP entries learned on an interface, in the range of 1 to 4,096. The default value is 1,024.

Description Use the **arp max-learning-num** command to set the maximum number of dynamic ARP entries that an interface can learn.

Use the **undo arp max-learning-num** command to restore the default.

Example # Set the maximum number of dynamic ARP entries that can be learned on VLAN-interface 40 to 500.

```
<Sysname> system-view
[Sysname] interface vlan-interface 40
[Sysname-Vlan-interface40]arp max-learning-num 500
```

arp static

Syntax **arp static** *ip-address mac-address* [*vlan-id interface-type interface-number*] [**vpn-instance** *vpn-instance-name*]

undo arp *ip-address* [**vpn-instance** *vpn-instance-name*]

View System view

Parameter *ip-address*: IP address in an ARP entry.

mac-address: MAC address in an ARP entry, in the format H-H-H.

vlan-id: ID of a VLAN to which a static ARP entry belongs to, in the range 1 to 4094.

interface-type interface-number: Interface type and interface number.

vpn-instance *vpn-instance-name*: Name of a VLAN instance, a case-sensitive string of 1 to 31 characters.

Description Use the **arp static** command to configure a static ARP entry in the ARP mapping table.

Use the **undo arp** command to remove an ARP entry.

Note that:

- A static ARP entry is effective when the device works normally. However, when the VLAN or VLAN interface to which an ARP entry corresponds is deleted, the entry, if permanent, will be deleted, and if non-permanent and resolved, will become unresolved.
- The *vlan-id* argument is used to specify the corresponding VLAN of an ARP entry and must be the ID of an existing VLAN. In addition, the Ethernet interfaces following the argument must belong to that VLAN. The VLAN interface of the VLAN must have been created.
- Before using the command with the **vpn-instance keyword** to configure a permanent static ARP entry, you need to create a VPN instance and bind it to the VLAN interface.

Related command: **reset arp**, **display arp**.

Example # Configure a static ARP entry, with the IP address being 202.38.10.2, the MAC address being 00e0-fc01-0000, and the outbound interface being Ethernet 1/0 of VLAN 10.

```
<Sysname> system-view
[Sysname] arp static 202.38.10.2 00e0-fc01-0000 10 ethernet 1/0
```

arp timer aging

Syntax **arp timer aging** *aging-time*

undo arp timer aging

View System view

Parameter *aging-time*: Aging time for dynamic ARP entries in minutes, in the range 1 to 1,440.

Description Use the **arp timer aging** command to set aging time for dynamic ARP entries.

Use the **undo arp timer aging** command to restore the default.

By default, the aging time for dynamic ARP entries is 20 minutes.

Related command: **display arp timer aging**.

Example # Set aging time for dynamic ARP entries to 10 minutes.

```
<Sysname> system-view
[Sysname] arp timer aging 10
```

display arp

Syntax **display arp** { { **all** | **dynamic** | **static** } | **vlan** *vlan-id* | **interface** *interface-type interface-number* } [[**verbose**] [| { **begin** | **exclude** | **include** } *string*] | **count**]

View Any view

Parameter **all**: Displays all ARP entries.

dynamic: Displays dynamic ARP entries.

static: Displays static ARP entries.

vlan *vlan-id*: Displays the ARP entries of the specified VLAN. The VLAN ID ranges from 1 to 4094.

interface *interface-type interface-number*: Displays the ARP entries of the interface specified by the argument *interface-type interface-number*.

verbose: Displays detailed information about ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries containing the specified string.

string: A case-sensitive string for matching, consisting of 1 to 256 characters.

count: Displays the number of ARP entries.

Description Use the **display arp** command to display ARP entries in the ARP mapping table.

Related command: **arp static**, **reset arp**.

Example # Display the detailed information of all ARP entries.

```
<Sysname> display arp all verbose
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface              Aging Type
Vpn-instance Name
20.1.1.1         00e0-fc00-0001  N/A      N/A                    N/A   S
test
193.1.1.70       00e0-fe50-6503  100      GE1/0                14    D
[No Vrf]
192.168.0.115    000d-88f7-9f7d  1        GE1/1                18    D
[No Vrf]
192.168.0.39     0012-a990-2241  1        GE1/2                20    D
[No Vrf]
```

Table 124 Description on the fields of the display arp command

Field	Description
IP Address	IP address in an ARP entry
MAC Address	MAC address in an ARP entry
VLAN ID	VLAN ID contained a static ARP entry
Interface	Outbound interface in an ARP entry
Aging	Aging time for a dynamic ARP entry in minutes
Type	ARP entry type: D stands for dynamic and S for static.
Vpn-instance Name	Name of VPN instance. [No Vrf] means no VPN instance is configured for the corresponding ARP.

Display the number of all ARP entries

```
<Sysname> display arp all count
Total Entry(ies): 4
```

display arp ip-address

Syntax **display arp** *ip-address* [**verbose**] [| { **begin** | **exclude** | **include** } *string*]

View Any view

Parameter *ip-address*: Displays the ARP entry for the specified IP address.

verbose: Displays the detailed information about ARP entries.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays the ARP entries from the first one containing the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

Include: Displays the ARP entries that contain the specified string.

string: A case-sensitive string for matching, consisting of 1 to 256 characters.

Description Use the **display arp** *ip-address* command to display the ARP entry for a specified IP address.

Related command: **arp static**, and **reset arp**.

Example # Display the corresponding ARP entry for the IP address 20.1.1.1.

```
<Sysname> display arp 20.1.1.1
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
20.1.1.1         00e0-fc00-0001  N/A      N/A                   N/A   S
```

display arp timer aging

Syntax **display arp timer aging**

View Any view

Parameter None

Description Use the **display arp timer aging** command to display the aging time for dynamic ARP entries.

Related command: **arp timer aging**.

Example # Display the aging time for dynamic ARP entries.

```
[Sysname] display arp timer aging
Current ARP aging time is 10 minute(s)
```

display arp vpn-instance

Syntax **display arp vpn-instance** *vpn-instance-name* [| { **begin** | **exclude** | **include** } *string* | **count**]

View Any view

Parameter *vpn-instance-name*: Name of VPN instance, a case-sensitive string of 1 to 31 characters. With this argument specified, the ARP entries for a specific VPN instance are displayed.

|: Uses a regular expression to specify the ARP entries to be displayed.

begin: Displays the ARP entries from the first one that contains the specified string.

exclude: Displays the ARP entries that do not contain the specified string.

include: Displays the ARP entries that contain the specified string.

string: A case-sensitive string for matching, consisting of 1 to 256 characters.

count: Displays the number of ARP entries.

Description Use the **display arp vpn-instance** command to display the ARP entries for a specified VPN instance.

Related command: **arp static** and **reset arp**.

Example # Display ARP entries for the VPN instance named test.

```
<Sysname> display arp vpn-instance test
                Type: S-Static    D-Dynamic
IP Address       MAC Address     VLAN ID  Interface             Aging Type
20.1.1.1         00e0-fc00-0001  N/A      N/A                   N/A   S
```

naturemask-arp enable

Syntax **naturemask-arp enable**

undo naturemask-arp enable

View System view

Parameter None

Description Use the **naturemask-arp enable** command to cancel the restriction that ARP requests must be from the same subnet. In this case, ARP requests from a natural network are supported.

Use the **undo naturemask-arp enable** command to restore the default.

By default, the support for ARP requests from a natural network is disabled.

Example # Enable the support for ARP requests from a natural network.

```
<Sysname> system-view
[Sysname] naturemask-arp enable
```

reset arp

Syntax **reset arp** { **all** | **dynamic** | **static** | **interface** *interface-type interface-number* }

View User view

Parameter **all:** Clears all ARP entries.

dynamic: Clears all dynamic ARP entries.

static: Clears all static ARP entries.

interface *interface-type interface-number*: Clears the ARP entries for the interface specified by the argument *interface-type interface-number*.

Description Use the **reset arp** command to clear ARP entries except authorized ARP entries from the ARP mapping table.

Note that with **interface** *interface-type interface-number* specified, the command clears only dynamic entries for the interface.

Related command: **arp static** and **display arp**.

Example # Clear all static ARP entries.

```
<Sysname> reset arp static
```

47 GRATUITOUS ARP CONFIGURATION COMMANDS

gratuitous-arp-sending enable

Syntax **gratuitous-arp-sending enable**

undo gratuitous-arp-sending enable

View System view

Parameter None

Description Use the **gratuitous-arp-sending enable** command to enable a device to send gratuitous ARP packets when receiving ARP requests from another network segment.

Use the **undo gratuitous-arp-sending enable** command to restore the default.

By default, a device cannot send gratuitous ARP packets when receiving ARP requests from another network segment.

Example # Disable a device from sending gratuitous ARP packets

```
<Sysname> system-view
[Sysname] undo gratuitous-arp-sending enable
```

gratuitous-arp-learning enable

Syntax **gratuitous-arp-learning enable**

undo gratuitous-arp-learning enable

View System view

Parameter None

Description Use the **gratuitous-arp-learning enable** command to enable the gratuitous ARP packet learning function.

Use the **undo gratuitous-arp-learning enable** command to disable the function.

By default, the function is disabled.

Example # Enable the gratuitous ARP packet learning function.

```
<Sysname> system-view
[Sysname] gratuitous-arp-learning enable
```

48 ARP SOURCE SUPPRESSION CONFIGURATION COMMANDS

arp source-suppression enable

Syntax **arp source-suppression enable**

undo arp source-suppression enable

View System view

Parameter None

Description Use the **arp source-suppression enable** command to enable the ARP source suppression function.

Use the **undo arp source-suppression enable** command to disable the function.

By default, the ARP source suppression function is disabled.

Related command: **display arp source-suppression**.

Example # Enable the ARP source suppression function.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname] arp source-suppression enable
```

arp source-suppression limit

Syntax **arp source-suppression limit** *limit-value*

undo arp source-suppression limit

View System view

Parameter *limit-value*: Specifies the maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds. It ranges from 2 to 1,024.

Description Use the **arp source-suppression limit** command to set the maximum number of packets with the same source IP address but unresolvable destination IP addresses that a port can receive in five seconds.

Use the **undo arp source-suppression limit** command to restore the default value, which is 10.

Related command: **display arp source-suppression**.

Example # Set to 100 the maximum number of packets with the same source address but unresolvable destination IP addresses that a port can receive in five seconds.

```
<Sysname> system-view
[Sysname] arp source-suppression limit 100
```

display arp source-suppression

Syntax **display arp source-suppression**

View Any view

Parameter None

Description Use the **display arp source-suppression** command to display information about the current ARP source suppression configuration.

Example # Display information about the current ARP source suppression configuration.

```
<Sysname> display arp source-suppression
 ARP source suppression is enabled
 Current suppression limit: 100
 Current cache length: 16
```

Table 125 Description on fields of display arp source-suppression

Field	Description
ARP source suppression is enabled	The ARP source suppression function is enabled.
Current suppression limit	Maximum number of packets with the same source IP address but unresolvable IP addresses that the device can receive in five seconds
Current cache length	Size of cache used to record source suppression information

49 AUTHORIZED ARP CONFIGURATION COMMANDS

This feature is supported on Layer 3 Ethernet interfaces only.

arp authorized enable

Syntax **arp authorized enable**

undo arp authorized enable

View Layer 3 Ethernet interface view

Parameter None

Description Use the **arp authorized enable** command to enable authorized ARP on an interface, which at the same time is enabled with authorized ARP aging detection but disabled from learning dynamic ARP entries.

Use the **undo arp authorized enable** command to disable authorized ARP on the interface, which at the same time is enabled to learn dynamic ARP entries.

By default, authorized ARP is not enabled on the interface.

Example # Enable authorized ARP on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] arp authorized enable
```

arp authorized time-out

Syntax **arp authorized time-out** *seconds*

undo arp authorized time-out

View Layer 3 Ethernet interface view

Parameter *seconds*: Aging time for authorized ARP entries in seconds, in the range 30 to 86400.

Description Use the **arp authorized time-out** command to configure the aging time for authorized ARP entries.

Use the **undo arp authorized time-out** command to restore the default.

By default, the aging time for authorized ARP entries is 1200 seconds.

Example # Configure the aging time for authorized ARP entries.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] arp authorized time-out 120
```

50 PROXY ARP CONFIGURATION COMMANDS

proxy-arp enable

Syntax **proxy-arp enable**

undo proxy-arp enable

View VLAN interface view/Ethernet interface view

Parameter None

Description Use the **proxy-arp enable** command to enable proxy ARP.

Use the **undo proxy-arp enable** command to disable proxy ARP.

By default, proxy ARP is disabled.

Related command: **display proxy-arp**.

Example # Enable proxy ARP on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] proxy-arp enable
```

local-proxy-arp enable

Syntax **local-proxy-arp enable**

undo local-proxy-arp enable

View VLAN interface view

Parameter None

Description Use the **local-proxy-arp enable** command to enable local proxy ARP.

Use the **undo local-proxy-arp enable** command to disable local proxy ARP.

By default, local proxy ARP is disabled.

Related command: **display local-proxy-arp**.

Example # Enable local proxy ARP on VLAN-interface 2.

```
<Sysname> system-view
[Sysname] interface Vlan-interface 2
[Sysname-Vlan-interface2] local-proxy-arp enable
```

display proxy-arp

Syntax **display proxy-arp** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Displays the proxy ARP status of the interface specified by the argument *interface-type interface-number*.

Description Use the **display proxy-arp** command to display the proxy ARP status.

Related command: **proxy-arp enable**.

Example # Display the proxy ARP status on Ethernet 1/0.

```
<Sysname> display proxy-arp interface ethernet 1/0
Interface Ethernet 1/0
 Proxy ARP status: disabled
```

display local-proxy-arp

Syntax **display local-proxy-arp** [**interface vlan-interface** *vlan-id*]

View Any view

Parameter **interface vlan-interface** *vlan-id*: Displays the local proxy ARP status of the specified VLAN interface.

Description Use the **display local-proxy-arp** command to display the status of the local proxy ARP.

Related command: **local-proxy-arp enable**.

Example # Display the status of the local proxy ARP on VLAN-interface 2.

```
<Sysname> display local-proxy-arp interface vlan-interface 2
Interface Vlan-interface2
 Local Proxy ARP status: enabled
```

51 DHCP SERVER CONFIGURATION COMMANDS

- *The DHCP server configuration is supported only on Layer 3 Ethernet interfaces (or subinterfaces), virtual Ethernet interfaces, VLAN interfaces, serial interfaces, and loopback interfaces. The subaddress pool configuration is not supported on serial and loopback interfaces.*
- *DHCP Snooping must be disabled on the DHCP server.*

bims-server

Syntax **bims-server ip** *ip-address* [**port** *port-number*] **sharekey** *key*

undo bims-server

View DHCP address pool view

Parameter **ip** *ip-address*: Specifies the IP address of a BIMS server.

port *port-number*: Specifies a port number for the BIMS server in the range 1 to 65534.

sharekey *key*: Specifies a shared key for the BIMS server, which is a string of 1 to 16 characters.

Description Use the **bims-server** command to specify the IP address, port number, and shared key of a BIMS server in the DHCP address pool for the client.

Use the **undo bims-server** command to remove specified BIMS server information from the DHCP address pool.

By default, the related information of the BIMS server is not specified.

If you execute the **bims-server** command repeatedly, the latest configuration will overwrite the previous one.

Related commands: **dhcp server ip-pool**.

Example # Specify the IP address 1.1.1.1, port number 80, shared key aabbcc of the BIMS server in DHCP address pool 0 for the client.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bims-server ip 1.1.1.1 port 80 sharekey aabbcc
```

bootfile-name

Syntax **bootfile-name** *bootfile-name*

undo bootfile-name

View DHCP address pool view

Parameter *bootfile-name*: Boot file name, a string of 1 to 63 characters.

Description Use the **bootfile-name** command to specify a bootfile name in the DHCP address pool for the client.

Use the **undo bootfile-name** command to remove the specified bootfile name from the DHCP address pool.

By default, no bootfile name is specified.

If you execute the **bootfile-name** command repeatedly, the latest configuration will overwrite the previous one.

Example # Specify the bootfile name aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] bootfile-name aaa
```

dhcp enable

Syntax **dhcp enable**

undo dhcp enable

View System view

Parameter None

Description Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

You need to enable DHCP before performing DHCP server and relay agent configurations.

Example # Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp select server global-pool

Syntax **dhcp select server global-pool** [**subaddress**]

undo dhcp select server global-pool subaddress

View Interface view

Parameter **subaddress**: Supports subaddress allocation. That is, the DHCP server and clients are on the same network segment, and the server allocates IP addresses from the address pool containing the network segment of the first subaddress if several subaddresses exist.

Description Use the **dhcp select server global-pool** command to enable the DHCP server on an interface. After the interface receives a DHCP request from the DHCP client, the DHCP server will allocate an IP address from the address pool.

Use the **undo dhcp select server global-pool subaddress** command to cancel the support for subaddress allocation.

By default, the DHCP server is enabled on an interface.

Example # Enable the DHCP server on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp select server global-pool
```

dhcp server detect

Syntax **dhcp server detect**

undo dhcp server detect

View System view

Parameter None

Description Use the **dhcp server detect** command to enable pseudo DHCP server detection.

Use the **undo dhcp server detect** command to disable the function.

By default, the function is disabled.

Example # Enable pseudo DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp server detect
```

dhcp server forbidden-ip

Syntax **dhcp server forbidden-ip** *low-ip-address* [*high-ip-address*]

undo dhcp server forbidden-ip *low-ip-address* [*high-ip-address*]

View System view

Parameter *low-ip-address*: Start IP address of the IP address range to be excluded from dynamic allocation.

high-ip-address: End IP address of the IP address range to be excluded from dynamic allocation. The end IP address must have a higher sequence than the start one.

Description Use the **dhcp server forbidden-ip** command to exclude IP addresses from dynamic allocation.

Use the **undo dhcp server forbidden-ip** command to remove the configuration.

By default, all IP addresses in a DHCP address pool are assignable except IP addresses of the DHCP server interfaces.

Note that:

- When you use the **dhcp server forbidden-ip** command to exclude an IP address that is bound to a user from dynamic assignment, the address can be still assigned to the user.
- When you use the **undo dhcp server forbidden-ip** command to remove the configuration, the specified address/address range must be consistent with the one specified in the **dhcp server forbidden-ip** command. If you have configured to exclude an address range from dynamic assignment, you need to specify an address range in the **undo dhcp server forbidden-ip** command instead of specifying one IP address.

Related command: **dhcp server ip-pool**, **network**, and **static-bind ip-address**.

Example # Exclude the IP address range 10.110.1.1 to 10.110.1.63 from dynamic allocation.

```
<Sysname> system-view
[Sysname] dhcp server forbidden-ip 10.110.1.1 10.110.1.63
```

dhcp server ip-pool

Syntax **dhcp server ip-pool** *pool-name*

undo dhcp server ip-pool *pool-name*

View System view

Parameter *pool-name*: Global address pool name, which is a unique pool identifier, a string of 1 to 35 characters.

Description Use the **dhcp server ip-pool** command to create a DHCP address pool and enter its view. If the pool was created, you will directly enter its view.

Use the **undo dhcp server ip-pool** command to remove specified DHCP address pool.

By default, no DHCP address pool is created.

Related command: **dhcp enable**.

Example # Create the DHCP address pool identified by 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0]
```

dhcp server ping packets

Syntax **dhcp server ping packets** *number*

undo dhcp server ping packets

View System view

Parameter *number*: Number of ping packets, in the range of 0 to 10. If the ping timeout time is set to 0, the DHCP server will not perform any ping collision detection.

Description Use the **dhcp server ping packets** command to specify the maximum number of ping packets on the DHCP server.

Use the **undo dhcp server ping packets** command to restore the default.

The number defaults to 1.

Example # Specify the maximum number of ping packets as 1.

```
<Sysname> system-view
[Sysname] dhcp server ping packets 10
```

dhcp server ping timeout

Syntax **dhcp server ping timeout** *milliseconds*

undo dhcp server ping timeout

View System view

Parameter *milliseconds*: Response timeout value for ping packets in milliseconds, in the range of 0 to 10,000. If the ping timeout time is set to 0, the DHCP server will not perform any ping collision detection.

Description Use the **dhcp server ping timeout** command to configure response timeout time of the ping packet on the DHCP server.

Use the **undo dhcp server ping timeout** command to restore the default.

The time defaults to 500.

Example # Specify the response timeout time as 1000ms.

```
<Sysname> system-view
[Sysname] dhcp server ping timeout 1000
```

dhcp server relay information enable

Syntax **dhcp server relay information enable**

undo dhcp server relay information enable

View System view.

Parameter None

Description Use the **dhcp server relay information enable** command to enable the DHCP server to handle option 82.

Use the **undo dhcp server relay information enable** command to disable the DHCP server from handling option 82.

By default, the DHCP server handles Option 82.

Example # Configure the DHCP server to ignore Option 82.

```
<Sysname> system-view
[Sysname] undo dhcp server relay information enable
```

dhcp update arp

Syntax **dhcp update arp**

undo dhcp update arp

View Interface view

Parameter None

Description Use the **dhcp update arp** command to configure the DHCP server to support authorized ARP.

Use the **undo dhcp update arp** command to restore the default.

By default, the DHCP server does not support authorized ARP.

Example # Configure Ethernet 1/0 to support authorized ARP.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp update arp
```

display dhcp server conflict

Syntax **display dhcp server conflict** { **all** | **ip** *ip-address* }

View Any view

Parameter **all**: Displays information about all IP address conflicts.

ip-address: Displays conflict information for the IP address.

Description Use the **display dhcp server conflict** command to display information about IP address conflicts.

Related command: **reset dhcp server conflict**.

Example # Display information about all IP address conflicts.

```
Address              Discover time
    4.4.4.1              Apr 25 2007 16:57:20
    4.4.4.2              Apr 25 2007 17:00:10
 --- total 2 entry ---
```

Table 126 Description on fields of the display dhcp server conflict command

Field	Description
Address	Conflicted IP address
Discover Time	Time when the conflict was discovered

display dhcp server expired

Syntax **display dhcp server expired** { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View Any view

Parameter **all**: Displays the lease expiration information of all DHCP address pools.

ip *ip-address*: Displays the lease expiration information of a specified IP address.

pool [*pool-name*]: Displays the lease expiration information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If the *pool name* is not specified, the lease expiration information of all address pools is displayed.

Description Use the **display dhcp server expired** command to display the lease expiration information of specified DHCP address pool(s) or an IP address.

DHCP will assign these expired IP addresses to DHCP clients after all addresses have been assigned.

Example # Display information about lease expirations in all DHCP address pools.

```
Global pool:
 IP address       Client-identifier/    Lease expiration          Type
                    Hardware address
 4.4.4.6          3030-3066-2e65-3230-  Apr 25 2007 17:10:47     Release
                   302e-3130-3234-2d45-
                   7468-6572-6e65-7430-
                   2f31
 --- total 1 entry ---
```

Table 127 Description on fields of the display dhcp server expired command

Field	Description
Global pool	Information about lease expiration of a DHCP address pool
IP address	Expired IP addresses
Client-identifier/Hardware address	IDs or MACs of clients whose IP addresses were expired
Lease expiration	The lease expiration time
Type	Types of lease expirations. Currently, this field is set to Release.

display dhcp server free-ip

Syntax **display dhcp server free-ip**

View Any view

Parameter None

Description Use the **display dhcp server free-ip** command to display information about assignable IP addresses, which have never been assigned.

Example # Display information about assignable IP addresses.

```
<Sysname> display dhcp server free-ip
IP Range from 10.0.0.0              to  10.0.0.255
```

display dhcp server forbidden-ip

Syntax **display dhcp server forbidden-ip**

View Any view

Parameter None

Description Use the **display dhcp server forbidden-ip** command to display IP addresses excluded from dynamic allocation in DHCP address pool.

Example # Display IP addresses excluded from dynamic allocation in the DHCP address pool.

```
<Sysname> display dhcp server forbidden-ip
IP Range from 1.1.1.1              to  1.1.1.1
IP Range from 2.2.2.2              to  2.2.2.5
```

display dhcp server ip-in-use

Syntax **display dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View Any view

Parameter **all**: Displays the binding information of all DHCP address pools.

ip *ip-address*: Displays the binding information of a specified IP address.

pool [*pool-name*]: Displays the binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the binding information of all address pools is displayed.

Description Use the **display dhcp server ip-in-use** command to display the binding information of DHCP address pool(s) or an IP address.

Related command: **reset dhcp server ip-in-use**.

Example # Display the binding information of all DHCP address pools.

```
<Sysname> display dhcp server ip-in-use all
 Global pool:
 IP address    Client-identifier/    Lease expiration        Type
                Hardware address
 10.1.1.1       4444-4444-4444        NOT Used              Manual

--- total 1 entry ---
```

Table 128 Description on fields of the display dhcp server ip-in-use command

Field	Description
Global pool	Binding information of a DHCP address pool
IP address	Bound IP address
Client-identifier/Hardware address	Client's ID or MAC of the binding
Lease expiration	Lease expiration time

Table 128 Description on fields of the display dhcp server ip-in-use command

Field	Description
Type	Binding types, including Manual, Auto:OFFERED and Auto:COMMITTED. ■ Manual: Static binding ■ Auto:OFFERED: The binding sent in the DHCP-OFFER message from the server to the client. ■ Auto:COMMITTED: The binding sent in the DHCP-ACK message from the server to the client.

display dhcp server statistics

Syntax **display dhcp server statistics**

View Any view

Parameter None

Description Use the **display dhcp server statistics** command to display the statistics of the DHCP server.

Related command: **reset dhcp server statistics**.

Example # Display the statistics on the DHCP server.

```
<Sysname> display dhcp server statistics
    Global Pool:
      Pool Number:                    1
      Binding:
        Auto:                          1
        Manual:                        0
        Expire:                        0
    BOOTP Request:                    13
      DHCPDISCOVER:                    3
      DHCPREQUEST:                     7
      DHCPDECLINE:                     0
      DHCPRELEASE:                     3
      DHCPINFORM:                      0
      BOOTPREQUEST:                    0
    BOOTP Reply:                      9
      DHCPOFFER:                       3
      DHCPACK:                         6
      DHCPNAK:                         0
      BOOTPREPLY:                      0
    Bad Messages:                     0
```

Table 129 Description on fields of the display dhcp server statistics command

Field	Description
Global Pool	Statistics of a DHCP address pool
Pool Number	The number of address pools
Auto	The number of dynamic bindings

Table 129 Description on fields of the display dhcp server statistics command

Field	Description
Manual	The number of static bindings
Expire	The number of expired bindings
BOOTP Request	The number of DHCP requests sent from DHCP clients to the DHCP server, including: ■ DHCPDISCOVER ■ DHCPREQUEST ■ DHCPDECLINE ■ DHCPRELEASE ■ DHCPINFORM ■ BOOTPREQUEST
BOOTP Reply	The number of DHCP replies sent from the DHCP server to DHCP clients, including: ■ DHCPOFFER ■ DHCPACK ■ DHCPNAK ■ BOOTPREPLY
Bad Messages	The number of erroneous messages

display dhcp server tree

Syntax **display dhcp server tree** { **all** | **pool** [*pool-name*] }

View Any view

Parameter **all**: Displays the tree organization information of all DHCP address pools.

pool [*pool-name*]: Displays the tree organization information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the tree organization information of all address pools will be displayed.

Description Use the **display dhcp server tree** command to display the tree organization information of DHCP address pool(s).

Example # Display the tree organization information of all DHCP address pools.

```
<Sysname> display dhcp server tree all
Global pool:

Pool name: 0
 network 20.1.1.0 mask 255.255.255.0
 Sibling node:1
 option 2 ip-address 1.1.1.1
 expired 1 0 0

Pool name: 1
 static-bind ip-address 10.10.1.2 mask 255.0.0.0
 static-bind mac-address 00e0-00fc-0001
```

```
PrevSibling node:0
expired unlimited
```

Table 130 Description on fields of the display dhcp server tree command

Field	Description
Global pool	Information of a address pool
Pool name	Address pool name
network	Network segment for address allocation
static-bind ip-address 10.10.1.2 mask 255.0.0.0	The IP address and MAC address of the static binding
static-bind mac-address 00e0-00fc-0001	
Sibling node	The sibling node of the current node, nodes of this kind in the output are: ■ Child node: The child node (subnet segment) address pool of the current node ■ Parent node: The parent node (nature network segment) address pool of the current node ■ Sibling node: The latter sibling node of the current node (another subnet of the same nature network). The earlier the sibling node is configured, the higher selection priority the sibling node has. ■ PrevSibling node: The previous sibling node of the current node
option	Self-defined DHCP options
expired	The lease duration, in the format of day, hour, and minute

dns-list

Syntax **dns-list** *ip-address*&<1-8>

undo dns-list { *ip-address* | **all** }

View DHCP address pool view

Parameter *ip-address*&<1-8>: DNS server IP address. &<1-8> means you can specify up to eight DNS server addresses separated by spaces.

all: Specifies all DNS server addresses to remove.

Description Use the **dns-list** command to specify DNS server addresses in a DHCP address pool.

Use the **undo dns-list** command to remove DNS server addresses from a DHCP address pool.

By default, no DNS server address is specified.

If you repeatedly use the **dns-list** command, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool**.

Example # Specify the DNS server address 10.1.1.254 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] dns-list 10.1.1.254
```

domain-name

Syntax **domain-name** *domain-name*

undo domain-name

View DHCP address pool view

Parameter *domain-name*: DHCP client domain name suffix, a string of 1 to 50 characters.

Description Use the **domain-name** command to specify the DHCP client domain name suffix in a DHCP address pool.

Use the **undo domain-name** command to remove the domain name suffix from a DHCP address pool.

The domain name suffix is not specified by default.

Related command: **dhcp server ip-pool**.

Example # Specify the client domain name suffix as mydomain.com in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] domain-name mydomain.com
```

expired

Syntax **expired** { **day** *day* [**hour** *hour* [**minute** *minute*]] | **unlimited** }

undo expired

View DHCP address pool view

Parameter **day** *day*: Specifies the number of days, in the range of 0 to 365.

hour *hour*: Specified the number of hours, in the range of 0 to 23.

minute *minute*: Specifies the number of minutes, in the range of 0 to 59.

unlimited: Specifies the infinite duration, which is actually 136 years.

Description Use the **expired** command to specify the lease duration in a DHCP address pool.

Use the **undo expired** command to restore the default lease duration in a DHCP address pool.

The lease duration defaults to one day.

Note that if the lease duration you specified is beyond the year 2106, the system regards the lease as expired.

Related command: **dhcp server ip-pool**.

Example # Specify the lease duration as one day, two hours and three minutes in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] expired day 1 hour 2 minute 3
```

gateway-list

Syntax **gateway-list** *ip-address*&<1-8>

undo gateway-list { *ip-address* | **all** }

View DHCP address pool view

Parameter *ip-address*&<1-8>: Gateway IP address. &<1-8> means you can specify up to eight gateway addresses separated by spaces.

all: Specifies all gateway IP addresses to be removed.

Description Use the **gateway-list** command to specify gateway address(es) in a DHCP address pool.

Use the **undo gateway-list** command to remove specified gateway address(es) from a DHCP address pool.

By default, no gateway address is specified.

If you use the **gateway-list** command repeatedly, the latest configuration will overwrite the previous one.

Example # Specify the gateway address 10.110.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] gateway-list 10.110.1.99
```

nbns-list

Syntax **nbns-list** *ip-address*&<1-8>

undo nbns-list { *ip-address* | **all** }

View DHCP address pool view

Parameter *ip-address*&<1-8>: WINS server IP address. &<1-8> means you can specify up to eight WINS server addresses separated by spaces.

all: Specifies all WINS server addresses to be removed.

Description Use the **nbns-list** command to specify WINS server address(es) in a DHCP address pool.

Use the **undo nbns-list** command to remove WINS server address(es) from a DHCP address pool.

By default, no WINS server address is specified.

If you use the **nbns-list** command repeatedly, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool** and **netbios-type**.

Example # Specify WINS server address 10.12.1.99 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] nbns-list 10.12.1.99
```

netbios-type

Syntax **netbios-type** { **b-node** | **h-node** | **m-node** | **p-node** }

undo netbios-type

View DHCP address pool view

Parameter **b-node**: Broadcast node. A b-node client sends the destination name in a broadcast message. The destination returns the name-to-IP mapping to the client after receiving the message.

p-node: Peer-to-peer node. A p-node client sends the destination name in a unicast message to the WINS server, and the WINS server returns the mapping to the client.

m-node: Mixed node, a combination of a b-node first and p-node second. An m-node client broadcasts the destination name, if there is no response, and then unicasts the destination name to the WINS server to get the mapping.

h-node: Hybrid node, a combination of a p-node first and b-node second. An h-node is a p-node with the peer-to-peer communication mechanism. An h-node client unicasts the destination name to the WINS server, if there is no response, and then broadcasts it to get the mapping from the destination.

Description Use the **netbios-type** command to specify the client NetBIOS node type in a DHCP address pool.

Use the **undo netbios-type** command to remove the client NetBIOS node type from a DHCP address pool.

No NetBIOS node type is specified by default.

Related command: **dhcp server ip-pool** and **nbns-list**.

Example # Specify the NetBIOS node type as b-node in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] netbios-type b-node
```

network

Syntax **network** *ip-address* [*mask-length* | **mask** *mask*]

undo network

View DHCP address pool view

Parameter *ip-address*: IP address range for dynamic allocation. If no mask length and mask is specified, the natural mask will be used.

mask-length: Mask length, in the range of 1 to 30.

mask *mask*: Specifies the IP address network mask, in dotted decimal notation.

Description Use the **network** command to specify the IP address range for dynamic allocation in a DHCP address pool.

Use the **undo network** command to remove the specified address range.

No IP address range is specified by default.

Note that you can specify only one network segment for each DHCP global address pool. If you use the **network** command repeatedly, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool** and **dhcp server forbidden-ip**.

Example # Specify 192.168.8.0/24 as the address range for dynamic allocation in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] network 192.168.8.0 mask 255.255.255.0
```

option

Syntax **option** *code* { **ascii** *ascii-string* | **hex** *hex-string*&<1-16> | **ip-address** *ip-address*&<1-8> }

undo option *code*

View DHCP address pool view

Parameter *code*: Self-defined option number, in the range of 2 to 254.

ascii *ascii-string*: Specifies an ASCII string with 1 to 63 characters.

hex *hex-string*&<1-16>: Specifies hex digit strings. &<1-16> indicates you can specify up to 16 hex digit strings, separated by spaces. Each string contains 2, 4, 6 or 8 hex digits.

ip-address *ip-address*&<1-8>: Specifies IP addresses. &<1-8> indicates you can specify up to eight IP addresses, separated by spaces.

Description Use the **option** command to configure a self-defined DHCP option in a DHCP address pool.

Use the **undo option** command to remove a self-defined DHCP option from a DHCP address pool.

The **option** command is not configured by default.

If you use the **option** command repeatedly, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool**.

Example # Configure the hex digits 0x11 and 0x22 for the self-defined DHCP option 100 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] option 100 hex 11 22
```

reset dhcp server conflict

Syntax **reset dhcp server conflict** { **all** | **ip** *ip-address* }

View User view

Parameter **all**: Clears the statistics of all IP address conflicts.

ip *ip-address*: Clears the conflict statistics of a specified IP address.

Description Use the **reset dhcp server conflict** command to clear statistics of IP address conflict(s).

Related command: **display dhcp server conflict**.

Example # Clear the statistics of all IP address conflicts.

```
<Sysname> reset dhcp server conflict all
```

reset dhcp server ip-in-use

Syntax **reset dhcp server ip-in-use** { **all** | **ip** *ip-address* | **pool** [*pool-name*] }

View User view

Parameter **all**: Clears the IP address dynamic binding information of all DHCP address pools.

ip *ip-address*: Clears the dynamic binding information of a specified IP address.

pool [*pool-name*]: Clears the dynamic binding information of a specified address pool. The *pool name* is a string of 1 to 35 characters. If no *pool name* is specified, the dynamic binding information of all address pools is cleared.

Description Use the **reset dhcp server ip-in-use** command to clear dynamic IP address binding information.

Related command: **display dhcp server ip-in-use**

Example # Clear the binding information of IP address 10.110.1.1.

```
<Sysname> reset dhcp server ip-in-use ip 10.110.1.1
```

reset dhcp server statistics

Syntax **reset dhcp server statistics**

View User view

Parameter None

Description Use the **reset dhcp server statistics** command to clear the statistics of the DHCP server.

Related command: **display dhcp server statistics**.

Example # Clear the statistics of the DHCP server.

```
<Sysname> reset dhcp server statistics
```

static-bind client-identifier

Syntax **static-bind client-identifier** *client-identifier*

undo static-bind client-identifier

View DHCP address pool view

Parameter *client-identifier*: The client ID of a static binding, a string with 4 to 160 characters in the format H-H-H..., each H indicates 4 hex digits except the last H indicates 2 or 4 hex digits. For example, aabb-cccc-dd is a valid ID, while aabb-c-dddd and aabb-cc-dddd are both invalid.

Description Use the **static-bind client-identifier** command to specify the client ID of a static binding in a DHCP address pool.

Use the **undo static-bind client-identifier** command to remove the client ID of a static binding from a DHCP address pool.

By default, no client ID is specified.

Note that:

- Use the **static-bind client-identifier** command together with the **static-bind ip-address** command to accomplish a static binding configuration.
- The ID of the static binding of a client must be identical to the ID displayed by using the **display dhcp client verbose** command on the client. Otherwise, the client cannot obtain an IP address.
- If you use the **static-bind client-identifier** or **static-bind mac-address** command repeatedly, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool**, **static-bind ip-address**, **static-bind mac-address**, and **display dhcp client verbose**.

Example # Bind the client ID aaaa-bbbb to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind client-identifier aaaa-bbbb
```

static-bind ip-address

Syntax **static-bind ip-address** *ip-address* [*mask-length* | **mask** *mask*]

undo static-bind ip-address

View DHCP address pool view

Parameter *ip-address*: IP address of a static binding, if no mask and mask length is specified, the natural mask is used.

mask-length: Mask length of the IP address, that is, the number of digit 1 in the mask.

mask *mask*: Specifies the IP address mask.

Description Use the **static-bind ip-address** command to specify the IP address of a static binding in a DHCP address pool.

Use the **undo static-bind ip-address** command to remove the IP address of a static binding from a DHCP address pool.

By default, no IP address of a static binding in a DHCP address pool is specified.

Note that:

- Use the **static-bind ip-address** command together with the **static-bind mac-address** or **static-bind client-identifier** command to accomplish a static binding configuration.
- If the IP address of a static binding is an interface address of the DHCP server, the static binding does not take effect.
- If you use the **static-bind ip-address** command repeatedly, the latest configuration will overwrite the previous one.

Related command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind mac-address**.

Example # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

static-bind mac-address

Syntax **static-bind mac-address** *mac-address*

undo static-bind mac-address

View DHCP address pool view

Parameter *mac-address*: The MAC address of a static binding, in the format H-H-H.

Description Use the **static-bind mac-address** command to specify the MAC address of a static binding in a DHCP address pool.

Use the **undo static-bind mac-address** command to remove the MAC address of a static binding from a DHCP address pool.

By default, no MAC address is specified.

Note that:

- Use the **static-bind mac-address** command together with the **static-bind ip-address** command to complete a static binding configuration.
- If you use the **static-bind mac-address** or **static-bind client-identifier** command repeatedly, the latest configuration will overwrite the previous one.

Relate command: **dhcp server ip-pool**, **static-bind client-identifier** and **static-bind ip-address.**

Example # Bind the client MAC address 0000-e03f-0305 to the IP address 10.1.1.1 with the mask 255.255.255.0 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] static-bind ip-address 10.1.1.1 mask 255.255.255.0
[Sysname-dhcp-pool-0] static-bind mac-address 0000-e03f-0305
```

tftp-server domain-name

Syntax **tftp-server domain-name** *domain-name*

undo tftp-server domain-name

View DHCP address pool view

Parameter *domain-name*: TFTP server name, a string of 1 to 63 characters.

Description Use the **tftp-server domain-name** command to specify a TFTP server name in a DHCP address pool.

Use the **undo tftp-server domain-name** command to remove the TFTP server name from a DHCP address pool.

By default, no TFTP server name is specified.

Using the **tftp-server domain-name** command repeatedly will overwrite the previous configuration.

Example # Specify the TFTP server name as aaa in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server domain-name aaa
```

tftp-server ip-address

Syntax **tftp-server ip-address** *ip-address*

undo tftp-server ip-address

View DHCP address pool view

Parameter *ip-address:* TFTP server IP address.

Description Use the **tftp-server ip-address** command to specify the TFTP server IP address in a DHCP address pool.

Use the **undo tftp-server ip-address** command to remove the TFTP server IP address from a DHCP address pool.

By default, no TFTP server address is specified.

Using the **tftp-server ip-address** command repeatedly will overwrite the previous configuration.

Example # Specify the TFTP server address 10.1.1.1 in DHCP address pool 0.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] tftp-server ip-address 10.1.1.1
```

voice-config

Syntax **voice-config** { **as-ip** *ip-address* | **fail-over** *ip-address dialer-string* | **ncp-ip** *ip-address* | **voice-vlan** *vlan-id* { **disable** | **enable** } }

undo voice-config [**as-ip** | **fail-over** | **ncp-ip** | **voice-vlan**]

View DHCP address pool view.

Parameter **as-ip** *ip-address*: Specifies IP address for the backup network calling processor.

fail-over *ip-address dialer-string*: Specifies the failover IP address and dialer string. The *dialer-string* is a string of 1 to 39 characters, which can be 0 to 9, and "*".

ncp-ip *ip-address*: Specifies IP address for the primary network calling processor.

voice-vlan *vlan-id*: Specifies the voice VLAN ID, in the range of 2 to 4094.

- **disable**: Disables the specified voice VLAN ID, meaning DHCP clients will not take this ID as their voice VLAN.
- **enable**: Enables the specified voice VLAN ID, meaning DHCP clients will take this ID as their voice VLAN.

Description Use the **voice-config** command to configure specified Option 184 contents in a DHCP address pool.

Use the **undo voice-config** command to remove specified option 184 contents from a DHCP address pool.

By default, no Option 184 content is configured.

Note that specifying the IP address of a network calling processor first is necessary to make other configured parameters take effect.

Example # Configure Option 184 in DHCP address pool 0: the primary network calling processor 10.1.1.1, backup network calling processor 10.2.2.2, voice VLAN ID 3 that is enabled, the failover IP address 10.3.3.3 and dialer string 99*.

```
<Sysname> system-view
[Sysname] dhcp server ip-pool 0
[Sysname-dhcp-pool-0] voice-config ncp-ip 10.1.1.1
[Sysname-dhcp-pool-0] voice-config as-ip 10.2.2.2
[Sysname-dhcp-pool-0] voice-config voice-vlan 3 enable
[Sysname-dhcp-pool-0] voice-config fail-over 10.3.3.3 99*
```

52 DHCP RELAY AGENT CONFIGURATION COMMANDS

- *The DHCP relay agent configuration is supported only on the Layer 3 Ethernet interface (or subinterface), virtual Ethernet interface, VLAN interface, and serial interface.*
- *DHCP Snooping cannot be configured on the DHCP relay agent.*

dhcp enable

Syntax **dhcp enable**

undo dhcp enable

View System view

Parameter None

Description Use the **dhcp enable** command to enable DHCP.

Use the **undo dhcp enable** command to disable DHCP.

By default, DHCP is disabled.

For both DHCP server and relay agent configuration, enabling DHCP first is necessary to make other configurations take effect.

Example # Enable DHCP.

```
<Sysname> system-view
[Sysname] dhcp enable
```

dhcp relay address-check

Syntax **dhcp relay address-check** { **disable** | **enable** }

View Interface view

Parameter **disable**: Disables IP address match checking on the relay agent.

enable: Enables IP address match checking on the relay agent.

Description Use the **dhcp relay address-check enable** command to enable IP address match check on the relay agent.

Use the **dhcp relay address-check disable** command to disable IP address match check on the relay agent.

By default, the function is disabled.

Note that this command can be executed only on Layer 3 Ethernet interfaces (including sub-interfaces) and VLAN interfaces.

Example # Enable IP address match checking on the DHCP relay agent.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp relay address-check enable
```

dhcp relay information enable

Syntax **dhcp relay information enable**

undo dhcp relay information enable

View Interface view

Parameter None

Description Use the **dhcp relay information enable** command to enable the relay agent to support option 82.

Use the **undo dhcp relay information enable** command to disable option 82 support.

By default, option 82 support is disabled on DHCP relay agent.

Example # Enable option 82 support on the relay agent.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp relay information enable
```

dhcp relay information format

Syntax **dhcp relay information format** { **normal** | **verbose** [**node-identifier** { **mac** | **sysname** | **user-defined** *node-identifier* }] }

undo dhcp relay information format [**verbose node-identifier**]

View Interface view

Parameter **normal**: Specifies the normal padding format.

verbose: Specifies the verbose padding format.

node-identifier { **mac** | **sysname** | **user-defined** *node-identifier* }: Specifies access node identifier. By default, the node MAC address is used as the node identifier.

- **mac** indicates using MAC address as the node identifier.
- **sysname** indicates using the device name of a node as the node identifier.
- **user-defined** *node-identifier* indicates using a specified character string as the node identifier, in which *node-identifier* is a string with 1 to 50 characters.

Description Use the **dhcp relay information format** command to specify a padding format for option 82.

Use the **undo dhcp relay information format** command to restore the default padding format.

The option 82 padding format defaults to **normal**.

- *Using the **undo dhcp relay information format** command without the keyword **verbose node-identifier** restores the default **normal** padding format, or with the keyword **verbose node-identifier** restores the **mac** mode of the **verbose** padding format.*
- *If configuring the handling strategy of the DHCP relay agent as **replace**, you need to configure a padding format of option 82. If the handling strategy is keep or drop, you need not configure any padding format.*
- *If sub-option 1 (node identifier) of Option 82 is padded with the device name (sysname) of a node, the device name must contain no spaces. Otherwise, the DHCP relay agent will drop the message.*

Example # Specify the verbose padding format for option 82.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp relay information enable
[Sysname-Ethernet1/0] dhcp relay information strategy replace
[Sysname-Ethernet1/0] dhcp relay information format verbose
```

dhcp relay information strategy

Syntax **dhcp relay information strategy** { **drop** | **keep** | **replace** }

undo dhcp relay information strategy

View Interface view

Parameter **drop**: Specifies to drop messages containing option 82.

keep: Specifies to forward messages containing option 82 without any change.

replace: Specifies to forward messages containing option 82 after replacing the original option 82 with the option 82 padded in the specified padding format.

Description Use the **dhcp relay information strategy** command to configure DHCP relay agent handling strategy for messages containing option 82.

Use the **undo dhcp relay information strategy** command to restore the default handling strategy.

The handling strategy for messages containing option 82 defaults to **replace**.

Example # Configure the DHCP relay agent handling strategy for messages containing option 82 as **keep**.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp relay information enable
[Sysname-Ethernet1/0] dhcp relay information strategy keep
```

dhcp relay release ip

Syntax **dhcp relay release** *ip client-ip*

View System view

Parameter *client-ip*: DHCP client IP address.

Description Use the **dhcp relay release ip** command to send a release request to a specified DHCP server for releasing a specified client IP address.

Example # Send a release request to the DHCP server for releasing the IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] dhcp relay release ip 1.1.1.1
```

dhcp relay security static

Syntax **dhcp relay security static** *ip-address mac-address* [**interface** *interface-type interface-number*]

undo dhcp relay security { *ip-address* | **all** | **dynamic** | **static** }

View System view

Parameter *ip-address*: Specifies a client IP address for creating a static binding.

mac-address: Specifies a client MAC address for creating a static binding, in the format H-H-H.

interface *interface-type interface-number*: Specifies a Layer 3 interface connecting to the DHCP client. *interface-type interface-number* specifies the interface type and interface number.

all: Specifies all entries of client IP-to-MAC bindings to be removed.

dynamic: Specifies entries of dynamic client IP-to-MAC bindings to be removed.

static: Specifies entries of manual client IP-to-MAC bindings to be removed.

Description Use the **dhcp relay security static** command to configure a static addressing binding, that is, the binding between IP address, MAC address, and Layer 3 interface on the relay agent.

Use the **undo dhcp relay security** command to remove specified binding entries from the relay agent.

No manual IP-to-MAC binding is configured on the DHCP relay agent by default.

Note that:

When using the **dhcp relay security static** command to bind an interface to a static binding entry, make sure that the interface is configured as a DHCP relay agent; otherwise, address entry conflicts may occur.

Related command: **display dhcp relay security**.

Example # Bind DHCP relay interface Ethernet 1/0 to IP address 10.10.1.1 and MAC address 0005-5d02-f2b3 of the client.

```
<Sysname> system-view
[Sysname] dhcp relay security static 10.10.1.1 0005-5d02-f2b3 interf
ace ethernet 1/0
```

dhcp relay security tracker

Syntax **dhcp relay security tracker** { *interval* | **auto** }

undo dhcp relay security tracker [*interval*]

View System view

Parameter *interval*: Refreshing interval in seconds, in the range of 1 to 120.

auto: Specifies the **auto** refreshing interval, which is the value of 60 seconds divided by the number of binding entries. Thus, the more entries are, the shorter interval is, but the shortest interval is no less than 500 ms.

Description Use the **dhcp relay security tracker** command to set a refreshing interval at which the relay agent contacts the DHCP server for refreshing dynamic bindings.

Use the **undo dhcp relay security tracker** command to restore the default interval.

The default handshake interval is **auto**, the value of 60 seconds divided by the number of binding entries.

Example # Set the handshake interval as 100 seconds.

```
<Sysname> system-view
[Sysname] dhcp relay security tracker 100
```

dhcp relay server-detect

Syntax **dhcp relay server-detect**

undo dhcp relay server-detect

View System view

Parameter None

Description Use the **dhcp relay server-detect** command to enable pseudo DHCP server detection.

Use the **undo dhcp relay server-detect** command to disable pseudo DHCP server detection.

By default, pseudo DHCP server detection is disabled.

Example # Enable pseudo DHCP server detection.

```
<Sysname> system-view
[Sysname] dhcp relay server-detect
```

dhcp relay server-group

Syntax **dhcp relay server-group** *group-* **ip** *ip-address*

undo dhcp relay server-group *group-id* [**ip** *ip-address*]

View System view

Parameter *group-id*: Specifies a DHCP server group number, in the range of 0 to 19.

ip *ip-address*: Specifies a DHCP server IP address.

Description Use the **dhcp relay server-group** command to specify a DHCP server for a DHCP server group.

Use the **undo dhcp relay server-group** command to remove a DHCP server from a DHCP server group, if no **ip** *ip-address* is specified, all servers in the DHCP server group and the server group itself will be removed.

By default, no DHCP server is specified for a DHCP server group.

Note that:

- The IP address of any DHCP server and any interface's IP address of the DHCP relay agent cannot be in the same network segment. Otherwise, the client may fail to obtain an IP address.
- If a server group has been correlated to multiple interfaces, you need to cancel these correlations before removing the server group.

Related command: **display dhcp relay server-group**.

Example # Specify DHCP server 1.1.1.1 for DHCP server group 1 on the relay agent.

```
<Sysname> system-view
[Sysname] dhcp relay server-group 1 ip 1.1.1.1
```

dhcp relay server-select

Syntax **dhcp relay server-select** *group-id*

undo dhcp relay server-select

View Interface view

Parameter *group-id*: Specifies a DHCP group number to be correlated, in the range of 0 to 19. The specified group must be an existing group containing at least a DHCP server.

Description Use the **dhcp relay server-select** command to correlate specified interface(s) to a specified DHCP server group.

Use the **undo dhcp relay server-select** command to remove a configured correlation.

By default, no DHCP server group is correlated with an interface on the relay agent.

Note that an interface on the relay agent can only be correlated to one DHCP server group, and a newly configured correlation overwrites the previous one. If the server group in the new correlation does not exist, the new configuration will not work. The interface still maintains the previous correlation.

Example # Correlate the interface Ethernet1/0 to the DHCP server group 1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp relay server-select 1
```

dhcp select relay

Syntax **dhcp select relay**

undo dhcp select relay

View Interface view

Parameter None

Description Use the **dhcp select relay** command to enable the relay agent on the current interface, specified or all interfaces. Upon receiving requests from an enabled interface, the relay agent will forward these requests to outside DHCP servers for IP address allocation.

Use the **undo dhcp select relay** command to restore the default on interface(s).

After DHCP is enabled, the DHCP server is enabled on an interface by default. That is, upon receiving a client's request from the interface, the DHCP server allocates an IP address from the DHCP address pool to the client.

When the working mode of the interface is changed from DHCP server to DHCP relay agent, neither the IP address leases nor the authorized ARP entries will be deleted. However, these ARP entries may conflict with the new static entries generated on the DHCP relay agent; therefore, you are recommended to delete the existing IP address leases when changing the interface working mode to DHCP relay agent.

Example # Enable the DHCP relay agent on the interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp select relay
```

dhcp update arp

Syntax **dhcp update arp**

undo dhcp update arp

View Interface view

Parameter None

Description Use the **dhcp update arp** command to configure the DHCP relay agent to support authorized ARP.

Use the **undo dhcp update arp** command to restore the default.

By default, the DHCP relay agent does not support authorized ARP.

Example # Configure Ethernet 1/0 to support authorized ARP.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp update arp
```

display dhcp relay

Syntax **display dhcp relay** { **all** | **interface** *interface-type interface-number* }

View Any view

Parameter **all**: Displays information of DHCP server groups that all interfaces correspond to.

interface *interface-type interface-number*: Displays information of the DHCP server group that a specified interface corresponds to.

Description Use the **display dhcp relay** command to display information about DHCP server groups correlated to an interface or all interfaces.

Example # Display information about DHCP server groups correlated to all interfaces.

```
[Sysname] display dhcp relay all
    Interface name            Server-group
    Ethernet1/1                   2
```

Table 131 Description on fields of the display dhcp relay all command

Field	Description
Interface name	Interface name
Server-group	DHCP server group number correlated to the interface.

display dhcp relay security

Syntax **display dhcp relay security** [*ip-address* | **dynamic** | **static**]

View Any view

Parameter *ip-address*: Displays the binding information of an IP address.

dynamic: Displays information about dynamic bindings.

static: Displays information about static bindings.

Description Use the **display dhcp relay security** command to display information about bindings of DHCP relay agents. If no parameter is specified, information about all bindings will be displayed.

Example # Display information about all bindings.

```
<Sysname> display dhcp relay security
IP Address      MAC Address     Type       Interface
 10.1.1.1       00e0-0000-0001  Static     Eth1/0
 10.1.1.5       00e0-0000-0000  Static     Vlan2
---   2 dhcp-security item(s) found   ---
```

Table 132 Description on fields of the display dhcp relay security command

Field	Description
IP Address	Client IP address
MAC Address	Client MAC address
Type	Type of binding, including dynamic and static
Interface	Layer 3 interface connecting to the DHCP client. If no interface is recorded in the binding entry, "N/A" is displayed.

display dhcp relay security statistics

Syntax **display dhcp relay security statistics**

View Any view

Parameter None

Description Use the **display dhcp relay security statistics** command to display statistics information about bindings of DHCP relay agents.

Example # Display statistics about client address binding entries.

```
<Sysname> display dhcp relay security statistics
Static Items      :1
Dynamic Items     :0
Temporary Items   :0
All Items          :1
```

Table 133 Description on fields of the display dhcp relay security statistics command

Field	Description
Static Items	Static client address binding items
Dynamic Items	Dynamic client address binding items
Temporary Items	Temporary client address binding items
All Items	All client address binding items

display dhcp relay security tracker

Syntax **display dhcp relay security tracker**

View Any view

Parameter None

Description Use the **display dhcp relay security tracker** command to display the interval for refreshing dynamic bindings on the relay agent.

Example # Display the interval for refreshing dynamic bindings on the relay agent.

```
[Sysname] display dhcp relay security tracker
Current tracker interval : Auto
```

The interval is 10 seconds.

display dhcp relay server-group

Syntax **display dhcp relay server-group** { *group-id* | **all** }

View Any view

Parameter *group-id*: Displays the information of the specified DHCP server group numbered from 0 to 19.

all: Displays the information of all DHCP server groups.

Description Use the **display dhcp relay server-group** command to display the configuration information of a specified or all DHCP server groups.

Example # Display IP addresses of DHCP servers in DHCP server group 1.

```
<Sysname> display dhcp relay server-group 1
    No.             Group IP
    1               1.1.1.1
    2               1.1.1.2
```

Table 134 Description on fields of the display dhcp relay server-group command

Field	Description
No.	Sequence number
Group IP	IP address in the server group

display dhcp relay statistics

Syntax **display dhcp relay statistics** [**server-group** { *group-id* | **all** }]

View Any view

Parameter *group-id*: Specifies a server group number in the range of 0 to 19 about which to display DHCP packet statistics.

all: Specifies all server groups about which to display DHCP packet statistics. Information for each group will be displayed.

Description Use the **display dhcp relay statistics** command to display DHCP packet statistics related to a specified or all DHCP server groups.

Note that if no parameter (**server-group** and **all)** is specified, all DHCP packet statistics on the relay agent will be displayed.

Example # Display all DHCP packet statistics on the relay agent.

```
<Sysname> display dhcp relay statistics
     Bad packets received:                  0
     DHCP packets received from clients:    20
         DHCPDISCOVER packets received:     10
         DHCPREQUEST packets received:      10
         DHCPINFORM packets received:       0
         DHCPRELEASE packets received:      0
         DHCPDECLINE packets received:      0
         BOOTPREQUEST packets:              0
     DHCP packets received from servers:    20
         DHCPOFFER packets received:        10
         DHCPACK packets received:          10
         DHCPNAK packets received:          0
         BOOTPREPLY packets:                0
     DHCP packets sent to servers:          20
     DHCP packets sent to clients:          20
```

Display DHCP packet statistics related to every server group on the relay agent.

```
<Sysname> display dhcp relay statistics server-group all
 DHCP relay server-group           #2
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                  5
     DHCPREQUEST                   5
     DHCPINFORM                        0
     DHCPRELEASE                   0
     DHCPDECLINE                   0
     BOOTPREQUEST                  0
 Server -> Client:
     DHCPOFFER                     5
     DHCPACK                       5
     DHCPNAK                       0
     BOOTPREPLY                    0

 DHCP relay server-group           #3
     Packet type               Packet number
 Client -> Server:
     DHCPDISCOVER                  5
     DHCPREQUEST                   5
     DHCPINFORM                        0
     DHCPRELEASE                   0
     DHCPDECLINE                   0
     BOOTPREQUEST                  0
 Server -> Client:
     DHCPOFFER                     5
     DHCPACK                       5
     DHCPNAK                       0
     BOOTPREPLY                    0
```

reset dhcp relay statistics

Syntax **reset dhcp relay statistics** [**server-group** *group-id*]

View User view

Parameter **server-group** *group-id*: Specifies a server group ID in the range of 0 to 19 about which to remove statistics from the relay agent.

Description Use the **reset dhcp relay statistics** command to remove statistics from the relay agent.

If no **server-group** is specified, all statistics will be removed from the relay agent.

Related command: **display dhcp relay statistics**.

Example # Remove all statistics from the DHCP relay agent.

```
<Sysname> reset dhcp relay statistics
```

53 DHCP CLIENT CONFIGURATION COMMANDS

- *The DHCP client configuration is supported only on the Layer 3 Ethernet interface (or subinterface) and VLAN interface.*
- *When multiple VLAN interfaces having the same MAC address use DHCP for IP address acquisition via a relay agent, the DHCP server cannot be the Windows 2000 Server or Windows 2003 Server.*
- *You are not recommended to enable both the DHCP client and the DHCP Snooping on the same device. Otherwise, DHCP Snooping entries may fail to be generated, or the DHCP client may fail to obtain an IP address.*

display dhcp client

Syntax **display dhcp client** [**verbose**] [**interface** *interface-type interface-number*]

View Any view

Parameter **verbose**: Specifies verbose DHCP client information to be displayed.

interface *interface-type interface-number*: Specifies an interface of which to display DHCP client information.

Description Use the **display dhcp client** command to display DHCP client information. If no **interface** *interface-type interface-number* is specified, DHCP client information of all interfaces will be displayed.

Example # Display DHCP client information of all interfaces.

```
<Sysname> display dhcp client
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 DHCP server: 40.1.1.2
```

Display verbose DHCP client information.

```
<Sysname> display dhcp client verbose
Vlan-interface1 DHCP client information:
 Current machine state: BOUND
 Allocated IP: 40.1.1.20 255.255.255.0
 Allocated lease: 259200 seconds, T1: 129600 seconds, T2: 226800 seconds
 Lease from 2005.08.13 15:37:59   to   2005.08.16 15:37:59
 DHCP server: 40.1.1.2
 Transaction ID: 0x1c09322d
 Default router: 40.1.1.2
```

```
 DNS server: 44.1.1.11
 DNS server: 44.1.1.12
 Domain name: ddd.com
Boot server: 200.200.200.200  1.1.1.1
Client ID: 3030-3066-2e65-3234-
           392e-3830-3438-2d56-
           6c61-6e2d-696e-7465-
           7266-6163-6531
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.
```

Table 135 Description on fields of the display dhcp client command

Field	Description
Vlan-interface1 DHCP client information	Information of the interface acting as the DHCP client
Current machine state	DHCP client current machine state
Allocated IP	The IP address allocated by the DHCP server
Allocated lease	The allocated lease time
T1	The 1/2 lease time (in seconds) of the DHCP client IP address
T2	The 7/8 lease time (in seconds) of the DHCP client IP address
Lease from....to....	The start and end time of the lease.
DHCP Server	DHCP server IP address that assigned the IP address
Transaction ID	Transaction ID, a random number chosen by the client to identify an IP address allocation.
Default router	The gateway address assigned to the client
DNS server	The DNS server address assigned to the client
Domain name	The domain name suffix assigned to the client
Boot server	PXE server addresses (up to 16 addresses) specified for the DHCP client, which are obtained through Option 43.
Client ID	Client ID
T1 will timeout in 1 day 11 hours 58 minutes 52 seconds.	How long the T1 (1/2 lease time) timer will timeout.

ip address dhcp-alloc

Syntax **ip address dhcp-alloc** [**client-identifier mac** *interface-type interface-number*]

undo ip address dhcp-alloc

View Interface view

Parameter **client-identifier mac** *interface-type interface-number*: Specifies the MAC address of an interface using which as the client ID to obtain an IP address.

Description Use the **ip address dhcp-alloc** command to configure an interface to use DHCP for IP address acquisition.

Use the **undo ip address dhcp-alloc** command to cancel an interface from using DHCP.

By default, an interface does not use DHCP for IP address acquisition.

Note that:

- If no parameter is specified, the client uses a character string comprised of the current interface name and MAC address as its ID for address acquisition.
- The DHCP client sends a DHCP-RELEASE message for releasing the IP address obtained via DHCP, if the interface of the client is down, the message cannot be sent.
- For a sub interface that obtained an IP address via DHCP, using the **shutdown** command on its primary interface does not make the DHCP client send a DHCP-RELEASE message for releasing the sub interface's IP address.

Example # Configure interface Ethernet 1/0 to use DHCP for IP address acquisition.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip address dhcp-alloc
```

- *The DHCP snooping is supported only on the Layer 2 Ethernet interface.*
- *DHCP Snooping supports no link aggregation. If a Layer 2 Ethernet interface is added into an aggregation group, DHCP Snooping configuration on it will not take effect. When the interface is removed from the group, DHCP Snooping can take effect.*
- *The DHCP snooping enabled device does not work if it is between the DHCP relay agent and DHCP server, and it can work when it is between the DHCP client and relay agent or between the DHCP client and server.*
- *The DHCP Snooping enabled device cannot be a DHCP server or DHCP relay agent.*
- *You are not recommended to enable the DHCP client, BOOTP client, and DHCP Snooping on the same device. Otherwise, DHCP Snooping entries may fail to be generated, or the BOOTP client/DHCP client may fail to obtain an IP address.*

Only the H3C MSR series routers installed with the 16-port or 24-port switching card support DHCP snooping.

54 DHCP SNOOPING CONFIGURATION COMMANDS

dhcp-snooping

Syntax **dhcp-snooping**

undo dhcp-snooping

View System view

Parameter None

Description Use the **dhcp-snooping** command to enable DHCP snooping.

Use the **undo dhcp-snooping** command to disable DHCP snooping.

With DHCP snooping disabled, all ports can forward responses from any DHCP servers and does not record binding information about MAC addresses of DHCP clients and the obtained IP addresses.

By default, DHCP snooping is disabled.

Related command: **display dhcp-snooping**.

Example # Enable DHCP snooping.

```
[Sysname] dhcp-snooping
```

dhcp-snooping trust

Syntax **dhcp-snooping trust**

undo dhcp-snooping trust

View Layer 2 Ethernet interface view

Parameter None

Description Use the **dhcp-snooping trust** command to set a port as trusted.

Use the **undo dhcp-snooping trust** command to restore the default state of a port.

All ports are untrusted by default.

Related command: **display dhcp-snooping trust**.

Example # Set port Ethernet 1/0 as trusted.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dhcp-snooping trust
```

display dhcp-snooping

Syntax **display dhcp-snooping**

View Any view

Parameter None

Description Use the **display dhcp-snooping** command to display the binding information recorded through DHCP snooping.

Related command: **dhcp-snooping**.

*Using the display **dhcp-snooping** command displays IP-to-MAC bindings that are present both in the DHCP-ACK and DHCP-REQUEST messages.*

Example # Display DHCP snooping address binding information.

```
<Sysname> display dhcp-snooping
 DHCP Snooping is enabled.
 The client binding table for all untrusted ports.
 Type : D--Dynamic , S--Static
 Type   IP Address       MAC Address         Lease          VLAN     Interface
 ====   ===============  ===============     ========== ==== =================
 D     10.1.1.1              00e0-fc00-0006   286   1    Ethernet1/0
 ---   1 dhcp-snooping item(s) found   ---
```

Table 136 Description on fields of the display dhcp snooping command

Field	Description
Type	Binding type
IP Address	IP address assigned to the DHCP client
MAC Address	MAC address of the DHCP client
Lease	Lease period of the IP address in seconds
VLAN	VLAN where the port connecting the DHCP client resides
Interface	Port to which the DHCP client is connected

display dhcp-snooping trust

Syntax **display dhcp-snooping trust**

View Any view

Parameter None

Description Use the **display dhcp-snooping trust** command to display information about trusted ports.

Related command: **dhcp-snooping trust**.

Example # Display information about trusted ports.

```
<Sysname> display dhcp-snooping trust
 DHCP Snooping is enabled.
 DHCP Snooping trust becomes active.
 Interface                                   Trusted
 ========================                  ============
 Ethernet1/0                                 Trusted
```

The above output shows that DHCP snooping is enabled, DHCP snooping trust is active, and port Ethernet 1/0 is trusted.

55 BOOTP CLIENT CONFIGURATION COMMANDS

- *BOOTP client configuration can only be used on Layer 3 Ethernet interfaces (including sub-interfaces) and VLAN interfaces.*
- *If several VLAN interfaces sharing the same MAC address obtain IP addresses through a BOOTP relay agent, the BOOTP server cannot be a Windows 2000 Server or Windows 2003 Server.*
- *You are not recommended to enable both the DHCP client and the DHCP Snooping on the same device. Otherwise, DHCP Snooping entries may fail to be generated, or the BOOTP client may fail to obtain an IP address.*

CAUTION: *The support for the DHCP Snooping function varies with devices.*

display bootp client

Syntax **display bootp client** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Displays the BOOTP client information of the interface.

Description Use the **display bootp client** command to display related information about a BOOTP client.

Note:

- If **interface** *interface-type interface-number* is not specified, the command will display information about BOOTP clients on all interfaces.
- If **interface** *interface-type interface-number* is specified, the command will display information about the BOOTP client on the specified interface.

Example # Display related information about the BOOTP client on Ethernet1/0.

```
<Sysname> display bootp client interface ethernet 1/0
Ethernet1/0 BOOTP client information:
Allocated IP: 169.254.0.2 255.255.0.0
Transaction ID = 0x3d8a7431
Mac Address  00e0-fc0a-c3ef
```

Table 137 Description on fields of the display bootp client command

Field	Description
Ethernet1/0 BOOTP client information or Vlan-interface1 BOOTP client information	Information of the interface serving as a BOOTP client
Allocated IP	BOOTP client's IP address allocated by the BOOTP server
Transaction ID	Value of the **XID** field in a BOOTP message, namely, a random number used to match a response message from the BOOTP server while the BOOTP client sends a BOOTP request to the BOOTP server. If the values of the **XID** field are different in the BOOTP response and request, the BOOTP client will drop the BOOTP response.
Mac Address	MAC address of a BOOTP client

ip address bootp-alloc

Syntax **ip address bootp-alloc**

undo ip address bootp-alloc

View Interface view

Parameter None

Description Use the **ip address bootp-alloc** command to enable an interface to obtain an IP address through BOOTP.

Use the **undo ip address bootp-alloc** command to disable the interface from obtaining an IP address through BOOTP.

By default, an interface does not obtain an IP address through BOOTP.

Related command: **display bootp client**.

Example # Configure Ethernet1/0 to obtain an IP address through BOOTP.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip address bootp-alloc
```

56 DHCP DEBUGGING COMMANDS

debugging dhcp server

Syntax **debugging dhcp server { all | error | event | packet }**

undo debugging dhcp server { all | error | event | packet }

View User view

Default Level 1: Monitor level

Parameters **all**: All types of debugging for DHCP server.

error: DHCP server error debugging.

event: DHCP server event debugging.

packet: DHCP server packet debugging.

Description Use the **debugging dhcp server** command to enable DHCP server debugging.

Use the **undo debugging dhcp server** command to disabled DHCP server debugging.

By default, DHCP server debugging is disabled.

Table 138 Description on the fields of the debugging dhcp server packet command

Field	Description
Rx/Tx	Receiving/sending operation
Interface *InterfaceName*	Receiving interface
Message type: *MessageType*	DHCP message type, that is, request or reply.
Hardware type: *HardwareType*	Hardware type of the DHCP client
Hardware address length: *HardwareAddressLength*	Hardware address length of the DHCP client
Hops: *Hops*	Hops that a DHCP message traveled
Transaction ID: *TransactionID*	A random number generated when the DHCP client initiates an application, which uniquely identifies an application process.
Seconds: *Seconds*	Time elapsed since the DHCP client initiated the application. It is not used currently, and its value is set to 0.

Table 138 Description on the fields of the debugging dhcp server packet command

Field	Description
Broadcast flag: *BroadcastFlag*	DHCP broadcast flag: 1 refers to broadcast, and 0 refers to unicast.
Your IP address: *YourIPAddress*	IP address that the DHCP server assigns to the client
Boot file name: *BootFileName*	Boot file name and path
DHCP message type: *DHCPmessagetype*	DHCP message type, which can be: ■ DHCP Discover ■ DHCP Offer ■ DHCP Request ■ DHCP Decline ■ DHCP ACK ■ DHCP NAK ■ DHCP Release ■ DHCP Inform

Table 139 Description on the fields of the debugging dhcp server event command

Field	Description
Sending ICMP ECHOREQUEST to target IP: *ip-address*.	An ICMP request is sent to verify whether the IP address is being used.
ICMP still need to detect for *time(s)* time(s).	The times for sending ICMP packets to detect the lease
Send *Message-Type* to *clientID/MAC* Offer IP=> *ip-address* via *ip-address*.	Succeeded in sending the DHCP packet
Failed to send *Message-Type* to *clientID/MAC*.	Failed to send the DHCP packet
Find manual binding lease successfully.	A static binding entry is found.
Assign *Lease-Type* Lease from global pool.	Assign a lease from the global address pool. The lease type can be Used, Free, and Timeout.
Reclaim conflicted IP Address from global pool.	Assign a lease from conflicted IP addresses in the global address pool
Lease is exhausted!	The lease duration expires.
Acknowledge the DHCPREQUEST message!	The DHCP server returns an ACK message and assigns the requested IP address to the client.
Deny DHCPREQUEST message!	The DHCP server returns an NAK message and does not assign the requested IP address to the client.

Table 140 Description on the fields of the debugging dhcp server error command

Field	Description
Dealing with packet failed!	Failed to process the DHCP packet
Decoding DHCP packet failed!	Failed to parse the DHCP packet
ucOp error!	DHCP packet type error
Building option failed!	Failed to create an option
No free buffer for option!	No free buffer space to create options
Deleting lease failed when manual binding!	Failed to delete the lease when configuring a static binding entry

Table 140 Description on the fields of the debugging dhcp server error command

Field	Description
Unable to generate *Message-Type* without an analyzed packet!	Failed to generate a packet without a parsed packet
Too many options have been configured!	Failed to generate a packet with too many options configured
Failed to cancel ICMP timer!	Failed to cancel the timer for sending ICMP packets
Failed to add ICMP timer!	Failed to add the timer for sending ICMP packets
Can not offer new IP without analyzed packet!	Failed to offer IP lease without the parsed packet
Fault occurs in DHCP Sever time interval!	The interval at which the DHCP server waits for client's response expires.

Examples # Configure DHCP server on the device, and enable all types of debugging for DHCP server. The DHCP client applies for IP address from the DHCP sever via a DHCP relay agent.

```
<Sysname> terminal debugging
<Sysname> debugging dhcp server all
*0.263828 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
 Checking for expired lease.
```

// Checking for an expired lease

```
*0.278312 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Receive DHCPDISCOVER from 00e0.fc14.1601-Vlan-interface2
 via 22.0.0.1.
*0.278312 Sysname DHCPS/7/DHCPS_DEBUG_PACKET:
Rx, interface Vlan-interface1
    Message type: request
    Hardware type: 1, Hardware address length: 6
    Hops: 1, Transaction ID: 4281385283
    Seconds: 0, Broadcast flag: 0
    Client IP address: 0.0.0.0    Your IP address: 0.0.0.0
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Discover
```

// A DHCP-DISCOVER packet received

```
*0.278312 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Sending ICMP ECHOREQUEST to target IP: 22.0.0.1.
*0.278312 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Assign Free Lease from global pool.
```

// Checking whether the IP address 22.0.0.1 is in use using ICMP before assigning it from the global address pool to the client.

```
*0.278406 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: ICMP ECHOREPLY received from Client IP 22.0.0.1.
*0.278406 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Create timeout timer for ICMP.
```

// The DHCP server receives a response from a client at 22.0.0.1, which indicates the IP address is in use.

```
*0.278406 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Sending ICMP ECHOREQUEST to target IP: 22.0.0.2.
```

// Checking whether the IP address 22.0.0.2 is in use

```
*0.278406 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Assign Free Lease from global pool.
*0.279016 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: ICMP Timeout!
*0.279016 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: ICMP detecting finished. The target IP can be used for d
hcp allocation.
```

// No ICMP reply is received from 22.0.0.2 after the timer expires, which indicates the IP address can be used for allocation.

```
*0.279016 Sysname DHCPS/7/DHCPS_DEBUG_PACKET:
Tx, interface Vlan-interface1
    Message type: reply
    Hardware type: 1, Hardware address length: 6
    Hops: 0, Transaction ID: 4281385283
    Seconds: 0, Broadcast flag: 0
    Client IP address: 0.0.0.0    Your IP address: 22.0.0.2
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Offer
```

// A DHCP-OFFER message containing the IP address 22.0.0.2 was sent to the DHCP client.

```
*0.279016 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DhcpServer: Send DHCPOFFER to 00e0.fc14.1601-Vlan-interface2 Offer I
P=> 22.0.0.2 via 22.0.0.1.
*0.279172 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Receive DHCPREQUEST from 00e0.fc14.1601-Vlan-interface2
via 22.0.0.1.
*0.279172 Sysname DHCPS/7/DHCPS_DEBUG_PACKET:
Rx, interface Vlan-interface1
    Message type: request
    Hardware type: 1, Hardware address length: 6
    Hops: 1, Transaction ID: 2294688324
    Seconds: 0, Broadcast flag: 0
    Client IP address: 0.0.0.0    Your IP address: 0.0.0.0
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Request
```

// A DHCP-REQUEST message received

```
*0.279172 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DHCPServer: Acknowledge the DHCPREQUEST message!
*0.279172 Sysname DHCPS/7/DHCPS_DEBUG_PACKET:
Tx, interface Vlan-interface1
```

```
    Message type: reply
    Hardware type: 1, Hardware address length: 6
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast flag: 0
    Client IP address: 0.0.0.0    Your IP address: 22.0.0.2
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Ack

*0.279172 Sysname DHCPS/7/DHCPS_DEBUG_COMMON:
DhcpServer: Send DHCPACK to 00e0.fc14.1601-Vlan-interface2 Offer IP=> 22.0.0
.2 via 22.0.0.1.
```

// Sending a DHCP-ACK message

debugging dhcp relay

Syntax **debugging dhcp relay** { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

undo debugging dhcp relay { **all** | **error** | **event** | **packet** [**client mac** *mac-address*] }

View User view

Default Level 1: Monitor level

Parameters **all**: All types of debugging for DHCP relay agent.

error: DHCP relay agent error debugging.

event: DHCP relay agent event debugging.

packet: DHCP relay agent packet debugging.

client mac *mac-address*: Debugging for packets that the DHCP relay agent forwards for a specific DHCP client. *mac-address* is the MAC address of the DHCP client, in the format of H-H-H.

Description Use the **debugging dhcp relay** command to enable DHCP relay agent debugging.

Use the **undo debugging dhcp relay** command to disable DHCP relay agent debugging.

By default, DHCP relay agent debugging is disabled.

Table 141 Description on the fields of the debugging dhcp relay packet command

Field	Description
RX/TX, *Message-Type*, interface *interfacename*.	Receiving or forwarding the message of the *Message-Type* type through the interface *interfacename*
Message type: *MessageType*	Content of the first byte in the DHCP message, that is, the DHCP message type, request or reply.

Table 141 Description on the fields of the debugging dhcp relay packet command

Field	Description
Hardware type: *HardwareType*	Hardware address type of the DHCP client. 1 refers to Ethernet type.
Your IP address: *YourIPAddress*	IP address that the DHCP server assigns to the client
DHCP message type: *DHCPmessagetype*	DHCP message type, which can be: ■ DHCP Discover ■ DHCP Offer ■ DHCP Request ■ DHCP Decline ■ DHCP ACK ■ DHCP NAK ■ DHCP Release ■ DHCP Inform

Table 142 Description on the fields of the debugging dhcp relay event command

Field	Description
interface	Forwarding interface configured with DHCP relay agent
CHardAddr	Hardware address of the DHCP client
Requesting security module(s) to delete all *entry-type* security entries succeeded.	Succeeded in requesting the security module(s) to delete all *entry-type* security entries. The *entry-type* can be dynamic or static.

Table 143 Description on the fields of the debugging dhcp relay error command

Field	Description
Dealing with option 82 failed!	Failed to process Option 82
Option82: parameter error!	Option number error of Option 82
Decoding DHCP packet failed!	Failed to parse the DHCP packet
Discard a BOOTP request packet because of too large hop count!	The hop count of the DHCP message reaches the maximum, and the message will be discarded.

Examples # The DHCP client obtains IP address from the DHCP server via a DHCP relay agent. Enable all types of debugging for the DHCP relay agent.

```
<Sysname> terminal debugging
<Sysname> debugging dhcp relay all
<Sysname>
*0.230094 Sysname DHCPR/7/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Discover packet.
*0.230094 Sysname DHCPR/7/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP request packet, interface Vlan-interface2.
*0.230094 Sysname DHCPR/7/DHCPR_DEBUG_PACKET:
From client to server(Server-group 0):
    Message type: request
    Hardware type: 1, Hardware address length: 6
    Hops: 1, Transaction ID: 4281385283
    Seconds: 0, Broadcast flag: 1
    Client IP address: 0.0.0.0    Your IP address: 0.0.0.0
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
```

```
    DHCP message type: DHCP Discover
*0.230094 Sysname DHCPR/7/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send request interface Vlan-interface22, dest IP: 11.0.0.1,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent received a DHCP-DISCOVER message from the DHCP client, and forwarded it to the DHCP server at 11.0.0.1 in DHCP server group 0.

```
*0.230891 Sysname DHCPR/7/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Offer packet.
*0.230891 Sysname DHCPR/7/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP reply packet, interface Vlan-interface22.

*0.230891 Sysname DHCPR/7/DHCPR_DEBUG_PACKET:
From server to client(Server-group 0):
    Message type: reply
    Hardware type: 1, Hardware address length: 6
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast flag: 1
    Client IP address: 0.0.0.0    Your IP address: 22.0.0.2
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Offer

*0.230891 Sysname DHCPR/7/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send reply interface Vlan-interface22, dest IP: 255.255.255.255,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent received a DHCP-OFFER message, and then broadcast it.

```
*0.230969 Sysname DHCPR/7/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Request packet.
*0.230969 Sysname DHCPR/7/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP request packet, interface Vlan-interface22.

*0.230969 Sysname DHCPR/7/DHCPR_DEBUG_PACKET:
From client to server(Server-group 0):
    Message type: request
    Hardware type: 1, Hardware address length: 6
    Hops: 1, Transaction ID: 2294688324
    Seconds: 0, Broadcast flag: 1
    Client IP address: 0.0.0.0    Your IP address: 0.0.0.0
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Request

*0.230969 Sysname DHCPR/7/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send request interface Vlan-interface22, dest IP: 11.0.0.1,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent received a DHCP-REQUEST message from the DHCP client, and forwarded it to the DHCP server at 11.0.0.1.

```
*0.231063 Sysname DHCPR/7/DHCPR_DEBUG_EVENT:
 Begin to deal with DHCP Ack packet.
*0.231063 Sysname DHCPR/7/DHCPR_DEBUG_PKTRXTX:
Rx, DHCP reply packet, interface Vlan-interface22.

*0.231063 Sysname DHCPR/7/DHCPR_DEBUG_PACKET:
From server to client(Server-group 0):
    Message type: reply
    Hardware type: 1, Hardware address length: 6
```

```
    Hops: 0, Transaction ID: 2294688324
    Seconds: 0, Broadcast flag: 1
    Client IP address: 0.0.0.0    Your IP address: 22.0.0.2
    Server IP address: 0.0.0.0    Relay agent IP address: 22.0.0.1
    Client hardware address: 00e0-fc14-1601
    Server host name: Not Configured, Boot file name: Not Configured
    DHCP message type: DHCP Ack

*0.231063 Sysname DHCPR/7/DHCPR_DEBUG_RELAYPKT:
Pkt Sent: send reply interface Vlan-interface22, dest IP: 255.255.255.255,
         CHardAddr: 00e0.fc14.1601, server-group: 0
```

// The DHCP relay agent received a DHCP-ACK message from the DHCP server, and then broadcast it.

debugging dhcp client

Syntax **debugging dhcp client** { **all** | **error** | **event** | **packet** }

undo debugging dhcp client { **all** | **error** | **event** | **packet** }

View User view

Default Level 1: Monitor level

Parameters **all**: All types of debugging for DHCP/BOOTP clients.

error: Error debugging or debugging for unknown packets of DHCP/BOOTP clients.

event: DHCP/BOOTP client event debugging.

packet: DHCP/BOOTP client packet debugging.

Description Use the **debugging dhcp client** command to enable DHCP/BOOTP client debugging.

Use the **undo debugging dhcp client** command to disable DHCP/BOOTP client debugging.

By default, the DHCP/BOOTP client debugging is disabled.

Table 144 Description on the fields of the debugging dhcp client packet command

Field	Description
InterfaceName: *operation*	Forwarding interface of the DHCP client
Head :	DHCP packet header
op(*operation-number*)	DHCP message type, where 1 refers to BOOTP request, and 2 refers to BOOT reply.
yiaddr(*YourIPAddress*)	IP address that the DHCP server assigns to the client
OptionsÔºö	Options field of the DHCP message, displayed in the original data format

Table 144 Description on the fields of the debugging dhcp client packet command

Field	Description
Decode option 43:	Original data in Option 43 of the received DHCP message
type(*DHCPmessagetype*)	DHCP message type, which can be: ■ DHCP Offer ■ DHCP ACK ■ DHCP NAK
mask(*subnet mask IP*)	Subnet mask assigned by the DHCP server
lease(*lease*)	Lease assigned by the DHCP server (in seconds)
T1Ô°à*T1*Ô°â	1/2 of the DHCP client's lease (in seconds)
T2Ô°à*T2*Ô°â	7/8 of the DHCP client's lease (in seconds)
server(*server-IP*)	IP address of the DHCP server that sends the packet
dns(*dns-server-ip*)	Domain name server address that the DHCP server assigns to the client
domain(*domain-name*)	Domain name suffix that the DHCP server assigns to the client
Boot server(*boot-server-ip*)	PXE server address list that the DHCP server assigns to the client with option 43

Table 145 Description on the fields of the debugging dhcp client event command

Field	Description
InterfaceName:	Interface of the DHCP client
FSM state transfer(*state1*-->*state2*) successfully.	The state of the DHCP client is changed from *state1* to *state2*.
Enabling/Disabling DHCP to CPU succeeded!	Succeeded in enabling/disabling the sending of DHCP message to CPU for processing
Notify route to add the default gateway *ip-address*.	Notifies the routing module to add a default route
Notify BIMS to connect: BIMS server ip = *ip-address*., port = *port*, sharekey = *sharekey*.	Notifies the BIMS module that a connection has been established
Move to BOUND state in *millisecond* milliseconds if no arp reply is received.	Changes to BOUND state within *millisecond* milliseconds if no ARP reply is received
Resend *Message-Type* for enough times! Wait for rebinding/Wait for expiring/Move to INIT state..	Finishes *Message-Type* packet retransmission, and waits for the rebinding/expiring state, or go to the INIT state

Table 146 Description on the fields of the debugging dhcp client error command

Field	Description
The interface is not ready!	The forwarding interface is not in the right state.
Can't set SO_SENDDATAIF on dhcp socket!	Failed to set the socket
Sending packet with socket failed!	Failed to send packets through the socket
Bind DHCP socket failure!	Failed to bind DHCP socket
Decoding options field failed!	Failed to parse the options field
Enabling/Disabling DHCP to CPU failed!	Failed to enable/disable the sending of DHCP message to CPU for processing

Table 146 Description on the fields of the debugging dhcp client error command

Field	Description
Warning: Deleting the interface information of specified interface failed!	Failed to delete the user information on the specified interface
Copying socket failed when send release packet!	Failed to copy the socket when sending the release packet
timer expired, but FSM state(*state*) is wrong!	The timer expires, but the current state of the DHCP client is wrong.
Skip parsing the current PXE server TLV in option 43 due to invalid server type.	Skip parsing the current PXE server address list in option 43 due to invalid PXE server type.
Skip parsing the current PXE server TLV in option 43 due to length error.	Skip parsing the current PXE server address list in option 43 due to invalid length of the PXE server address list.
Skip parsing the current PXE server TLV in option 43 due to invalid server number.	Skip parsing the current PXE server address list in option 43 due to invalid PXE server number.
Skip parsing the current PXE server TLV in option 43 due to unknown error.	Skip parsing the current PXE server address list in option 43 due to unknown error.

Examples # The DHCP client obtains IP address from the DHCP server via a DHCP relay agent. Enable all types of debugging for the DHCP client.

```
<Sysname> debugging dhcp client all
<Sysname> terminal debugging
<Sysname> system
[Sysname] interface vlan-interface 2
[Sysname-Vlan-interface2] ip address dhcp-alloc
[Sysname-Vlan-interface2]
*0.105343 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2:
Enabling DHCP to CPU succeeded!
```

// The interface obtained an IP address through DHCP successfully. The DHCP message will be sent to the CPU for processing.

```
*0.105359 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Move to INIT state.
*0.105359 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: FSM state transfer(HALT-->INIT) successfully.
```

// The state of the DHCP client is changed from HALT to INIT.

```
*0.105359 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Send DHCPDISCOVER in 5 seconds.
*0.110343 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Send a Dhcp packet...
  Head : op(1); htype(ETHERNET); hlen(6); xid(0x43c130ff);
    ciaddr(0.0.0.0); yiaddr(0.0.0.0); chaddr(00e0-fc14-1601);
  Options :
    63 82 53 63 35 01 01 0C 06 63 6C 69 65 6E 74 37
    04 01 03 06 0F 39 02 04 80 3C 10 00 00 00 00 20
    B8 C4 B1 E4 B5 B1 C7 B0 C2 B7 BE 3D 20 00 30 30
    65 30 2E 66 63 31 34 2E 31 36 30 31 2D 56 6C 61
    6E 2D 69 6E 74 65 72 66 61 63 65 32 32 FF
```

```
*0.110343 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Sending DHCPDISCOVER packet succeeded.
*0.110343 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: FSM state transfer(INIT-->SELECTING) successfully.
```

// The DHCP client sent the DHCP-DISCOVER message successfully, and the state of the DHCP client is changed from INIT to SELECTING.

```
*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Receive a packet.
*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Receive a DHCP packet...
  Head : op(BOOTPREPLY); htype(ETHERNET); hlen(6); xid(0x43c130ff);
    ciaddr(0.0.0.0); yiaddr(22.0.0.2); chaddr(00e0-fc14-1601);
  Option : type(DHCPOFFER); mask(255.255.255.0); lease(86400);
    T1(43200); T2(75600); server(11.0.0.1);
*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Select 11.0.0.1 as the server.
```

// The DHCP client received a DHCP-OFFER message from the DHCP server at 11.0.0.1. The assigned IP address is 22.0.0.2, and the lease period is 86400 seconds (one day).

```
*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Send a Dhcp packet...
  Head : op(1); htype(ETHERNET); hlen(6); xid(0x442ac688);
    ciaddr(0.0.0.0); yiaddr(0.0.0.0); chaddr(00e0-fc14-1601);
  Options :
    63 82 53 63 35 01 03 0C 06 63 6C 69 65 6E 74 32
    04 16 00 00 02 36 04 0B 00 00 01 37 04 01 03 06
    0F 39 02 04 80 3C 10 00 00 00 00 44 65 63 00 4E
    6F 76 00 4F 63 74 00 3D 20 00 30 30 65 30 2E 66
    63 31 34 2E 31 36 30 31 2D 56 6C 61 6E 2D 69 6E
    74 65 72 66 61 63 65 32 32 FF

*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Sending DHCPREQUEST packet succeeded.
*0.111218 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: FSM state transfer(SELECTING-->REQUESTING) successfully.
```

// The DHCP client sent the DHCP-REQUEST message successfully, and the state of the DHCP client is changed from SELECTING to REQUESTING.

```
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Receive a packet.
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Receive a DHCP packet...
  Head : op(BOOTPREPLY); htype(ETHERNET); hlen(6); xid(0x442ac688);
    ciaddr(0.0.0.0); yiaddr(22.0.0.2); chaddr(00e0-fc14-1601);
  Option : type(DHCPACK); mask(255.255.255.0); lease(86400);
    T1(43200); T2(75600); server(11.0.0.1);
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: FSM state transfer(REQUESTING-->BOUND) successfully.
```

// The DHCP client received a DHCP-ACK message, and the state of the DHCP client is changed from REQUESTING to OUND.

```
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Begin to detect IP address conflict via ARP.
```

// The DHCP client starts address conflict detection using ARP.

```
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Sending arp request for allocated address(22.0.0.2)
succeeded.
```

// ARP message sent

```
*0.111421 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Move to BOUND state in 1 seconds if no arp reply is received.
```

// If no ARP reply is received, the state of the DHCP client will be changed to BOUND state after 1 second.

```
*0.112375 Sysname DHCPC/7/DHCP_Client:
Vlan-interface2: Receive no arp reply for 22.0.0.2, begin to use the address.
```

// Since no ARP reply is received, the state of the DHCP client is changed to BOUND, and the IP address can be used.

57 DNS CONFIGURATION COMMANDS

This document only covers IPv4 DNS configuration commands. For IPv6 DNS configuration commands, refer to "IPv6 Basics Configuration Commands" on page 829.

display dns domain

Syntax **display dns domain** [**dynamic**]

View Any view

Parameter **dynamic**: Displays the domain name suffixes dynamically obtained through DHCP or other protocols.

Description Use the **display dns domain** command to display the domain name suffixes.

Related command: **dns domain**.

Example # Display domain name suffixes.

```
<Sysname> display dns domain
 Type:
  D:Dynamic    S:Static

No.     Type    Domain-name
1       S       com
```

Table 147 Description on fields of display dns domain command

Field	Description
No	Sequence number
Type	Type of domain name suffix: S represents a statically configured domain name suffix, and D represents a domain name suffix obtained dynamically through DHCP.
Domain-name	Domain name suffix

display dns dynamic-host

Syntax **display dns dynamic-host**

View Any view

Parameter None

Description Use the **display dns dynamic-host** command to display the information in the dynamic domain name resolution cache.

Example # Display the information in the dynamic domain name resolution cache.

```
<Sysname> display dns dynamic-host
No  Host                  IP Address            TTL
1   www.baidu.com         202.108.249.134      63000
2   www.yahoo.akadns.net  66.94.230.39         24
3   www.hotmail.com       207.68.172.239       3585
4   www.eyou.com          61.136.62.70         3591
```

Table 148 Description on the field of the display dns dynamic-host command

Field	Description
No	Sequence number
Host	Domain name
IP Address	IP address for the corresponding domain name
TTL	Time a mapping can be stored in the cache (seconds).

*The domain-name field in the **display dns dynamic-host** command contains 21 characters at most. If a resolved domain name consists of more than 21 characters, only the first 21 characters are displayed.*

display dns proxy table

Syntax **display dns proxy table**

View Any view

Parameters None

Description Use the **display dns proxy table** command to display the DNS proxy table.

Examples # Display the DNS proxy table.

```
<Sysname> display dns proxy table
Source IP          Source Port  Trans ID     Server IP          Aging
192.168.0.98       1030         24580        192.168.111.244    35
```

Table 149 Description on the fields of the display dns proxy table command

Field	Description
Source IP	Source IP address of the DNS request, that is, the IP address of the DNS client.
Source Port	Source port number of the DNS request
Trans ID	Transaction ID of the DNS request
Server IP	IP address of the DNS server
Aging	Aging time of the DNS proxy table entry

display dns server

Syntax **display dns server** [**dynamic**]

View Any view

Parameter **dynamic**: Displays the DNS server information dynamically obtained through DHCP or other protocols

Description Use the **display dns server** command to display the DNS server information.

Related command: **dns server**.

Example # Display the DNS server information.

```
<Sysname> display dns server
Type:
  D:Dynamic    S:Static

DNS Server  Type  IP Address
    1       S     169.254.65.125
```

Table 150 Description on fields of the display dns server command

Field	Description
DNS Server	Sequence number of the DNS server. Configured automatically by the device, starting from 1.
Type	Type of domain name server: S represents a statically configured DNS server, and D represents a DNS server obtained dynamically through DHCP.
IP Address	IP address of the DNS server

display ip host

Syntax **display ip host**

View Any view

Parameter None

Description Use the **display ip host** command to display the host names and corresponding IP addresses in the static DNS database.

Example # Display the host names and corresponding IP addresses in the static DNS database.

```
<Sysname> display ip host
Host            Age     Flags       Address
My          0       static      1.1.1.1
Aa          0       static      2.2.2.4
```

Table 151 Description on fields of the display ip host command

Field	Description
Host	Host name
Age	Time to live. 0 means that a static mapping will never age out.
	You can only manually remove the mappings between host names and IP addresses.
Flags	Indicates the type of mappings between host names and IP addresses, static or dynamic.
	Static represents static domain name resolution.
Address	Host IP addresses

dns domain

Syntax **dns domain** *domain-name*

undo dns domain [*domain-name*]

View System view

Parameter *domain-name*: Domain name suffix, which is case-insensitive and consists of character strings separated by a dot (for example, aabbcc.com). Each separated string contains no more than 63 characters. The length of a domain name suffix with dots included is up to 238 characters. Character strings can contain letters, digits, hyphens (-), underscores (_), and dots (.).

Description Use the **dns domain** command to configure a domain name suffix.

Use the **undo dns domain** command to delete a domain name suffix (with a domain name suffix specified) or all domain name suffixes (with no domain name suffix specified).

No domain name suffix is configured by default.

You can configure a maximum of 10 domain name suffixes.

Related command: **display dns domain**.

Example # Configure com as a DNS suffix.

```
[Sysname] dns domain com
```

dns proxy enable

Syntax **dns proxy enable**

undo dns proxy enable

View System view

Parameters None

Description Use the **dns proxy enable** command to enable DNS proxy.

Use the **undo dns proxy enable** command to disable DNS proxy.

By default, DNS proxy is disabled.

Examples # Enable DNS proxy.

```
<Sysname> system-view
[Sysname] dns proxy enable
```

dns resolve

Syntax **dns resolve**

undo dns resolve

View System view

Parameter None

Description Use the **dns resolve** command to enable dynamic domain name resolution.

Use the **undo dns resolve** command to disable dynamic domain name resolution.

Dynamic domain name resolution is disabled by default.

Example # Enable dynamic domain name resolution.

```
[Sysname] dns resolve
```

dns server

Syntax **dns server** *ip-address*

undo dns server [*ip-address*]

View System view

Parameter *ip-address*: IP address of the DNS server.

Description Use the **dns server** command to configure an IP address for the DNS server.

Use the **undo dns server** to remove the IP address.

No IP address is configured for the DNS server by default.

You can configure a maximum of six DNS servers.

Related command: **display dns server**.

For details about IPv6 DNS, refer to "IPv6 Basics Configuration Commands" on page 829.

Example # Configure 172.16.1.1 for the DNS server.

```
[Sysname] dns server 172.16.1.1
```

ip host

Syntax **ip host** *hostname ip-address*

undo ip host *hostname* [*ip-address*]

View System view

Parameter *Hostname*: Host name, consisting of 1 to 20 characters, including case-insensitive letters, numbers, hyphens (-), or dots (.). The host name must include at least one letter.

ip-address: IP address of the specified host in dotted decimal notation.

Description Use the **ip host** command to create a mapping between host name and IP address in the static resolving list.

Use the **undo ip host** command to remove the mapping.

No mappings are created by default.

You can configure only one mapping between IP address and host name. For example, a mapping configured last time will overwrite the previous one if there is any.

Related command: **display ip host**.

Example # Configure the IP address 10.110.0.1 for a host named **aaa**.

```
[Sysname] ip host aaa 10.110.0.1
```

reset dns dynamic-host

Syntax **reset dns dynamic-host**

View User view

Parameter None

Description Use the **reset dns dynamic-host** command to clear the information in the dynamic domain name cache.

Related command: **display dns dynamic-host**.

Example # Clear the information in the dynamic domain name cache.

```
<Sysname> reset dns dynamic-host
```

58 IP ACCOUNTING CONFIGURATION COMMANDS

display ip count

Syntax **display ip count { inbound-packets | outbound-packets } { exterior | firewall-denied | interior }**

View Any view

Parameter **inbound-packets**: Displays information about incoming IP packets.

outbound-packets: Displays information about outgoing IP packets.

exterior: Displays information about the IP packets in the exterior table. The exterior table records rule-incompliant packets.

firewall-denied: Displays information about denied IP packets.

interior: Displays information about the IP packets in the interior table. The interior table records rule-compliant packets.

If no firewall is configured on the interface, packets refer to all incoming and outgoing IP packets. If a firewall is configured, only those valid packets can pass the firewall.

Description Use the **display ip count** command to display the statistics of the IP accounting about IP packets.

Example # Display information about valid rule-incompliant incoming IP packets.

```
<Sysname> display ip count inbound-packets exterior
6 Inbound streams information in exterior list:
  SrcIP            DstIP               Protocol  Pkts        Bytes
  0.0.0.0          255.255.255.255     UDP       28          9502
  10.153.72.181    10.153.73.255       UDP       174         38034
  10.153.72.137    239.255.255.250     UDP       4           644
  10.153.72.141    224.0.0.2           IGMP      4           128
  10.153.72.141    224.0.0.9           UDP       4           208
  10.153.72.141    224.0.0.9           IGMP      4           128
```

Table 152 Description on the fields of the display ip count command

Field	Description
SrcIP	Source IP address of a packet
DstIP	Destination IP address of a packet

Table 152 Description on the fields of the display ip count command

Field	Description
Protocol	Protocol carried in a packet
Pkts	Number of packets
Bytes	Number of bytes of packets

display ip count rule

Syntax **display ip count rule**

View Any view

Parameter None

Description Use the **display ip count rule** command to display IP accounting rules.

Example # Display IP accounting rules.

```
<Sysname> display ip count rule
 IP Count rule list:
   IP address     address mask
   1.1.1.0         255.255.255.0
   2.0.0.0         255.0.0.0
 -----------------------------------
 Total: 2 rules
```

Table 153 Description on fields of the display ip count rule command

Field	Description
IP address	IP address
address mask	Subnet mask

ip count enable

Syntax **ip count enable**

undo ip count enable

View System view

Parameter None

Description Use the **ip count enable** command to enable IP accounting.

Use the **undo ip count enable** command to disable IP accounting.

By default, IP accounting is disabled.

Example # Enable IP accounting.

```
<Sysname> system-view
[Sysname] ip count enable
```

ip count exterior-threshold

Syntax **ip count exterior-threshold** *number*

undo ip count exterior-threshold

View System view

Parameter *number*: Maximum number of accounting entries in the exterior table, in the range of 0 to 8,192.

Description Use the **ip count exterior-threshold** command to configure the maximum number of accounting entries in the exterior table.

Use the **undo ip count exterior-threshold** command to restore the default. When doing this, you are prompted to clear the table first if any accounting entries already exist in the table.

By default, the maximum number of accounting entries in the exterior table is 0. Rule-incompliant packets are not to be counted.

IP packets are sorted as follows:

- If a firewall is configured on an interface and incoming and outgoing IP packets are denied by the firewall, these IP packets are counted in the firewall-denied table.
- If the source or destination IP address of the IP packets passing the interface (in this case, a firewall may be configured or not) matches a network address in the IP accounting rule, the packets are recorded in the interior table. Otherwise, the packets are counted in the exterior table.

Example # Set the maximum number of accounting entries in the exterior table to 100.

```
<Sysname> system-view
[Sysname] ip count exterior-threshold 100
```

ip count firewall-denied

Syntax **ip count firewall-denied** { **inbound-packets** | **outbound-packets** }

undo ip count firewall-denied { **inbound-packets** | **outbound-packets** }

View Interface view

Parameter **inbound-packets**: Counts the incoming IP packets denied by the firewall on the current interface.

outbound-packets: Counts the outgoing IP packets denied by the firewall on the current interface.

Description Use the **ip count firewall-denied** command to count the IP packets denied by the firewall on the current interface.

Use the **undo ip count firewall-denied** command to restore the default.

By default, IP packets denied by the firewall are not counted.

Information about counted firewall-denied IP packets is stored in the firewall-denied table.

Example # Count the outgoing IP packets denied by the firewall on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip count firewall-denied outbound-packets
```

Specify not to count the outbound IP packets denied by the firewall on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo ip count firewall-denied outbound-packets
```

ip count inbound-packets

Syntax **ip count inbound-packets**

undo ip count inbound-packets

View Interface view

Parameter None

Description Use the **ip count inbound-packets** command to count incoming IP packets on the current interface.

Use the **undo ip count inbound-packets** command to restore the default.

By default, incoming IP packets on the interface are not counted.

After you execute the **ip count inbound-packets** command in interface view, the incoming IP packets are stored in the exterior or interior table, depending on whether they match the IP accounting rules.

If no firewall is configured on the interface, valid packets refer to all incoming and outgoing IP packets. If a firewall is configured, valid packets refer to only those passing the firewall.

Example # Count incoming IP packets on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip count inbound-packets
```

Specify not to count incoming IP packets on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo ip count inbound-packets
```

ip count interior-threshold

Syntax **ip count interior-threshold** *number*

undo ip count interior-threshold

View System view

Parameter *number*: Maximum number of accounting entries in the interior table, in the range 0 to 16,384.

Description Use the **ip count interior-threshold** command to configure maximum number of accounting entries in the interior table.

Use the **undo ip count interior-threshold** command to restore the default. When doing this, you are prompted to clear the table first if the number of accounting entries in the table is greater than the default.

By default, maximum number of accounting entries in the interior table is 512.

IP packets are sorted as follows:

- If a firewall is configured on an interface and incoming and outgoing IP packets are denied by the firewall, these IP packets are recorded in the firewall-denied table.
- If the source or destination IP address of the IP packets passing the interface (in this case, a firewall may be configured or not) matches a network address in the IP accounting rule, the packets are recorded in the interior table. Otherwise, the packets are recorded in the exterior table.

Example # Set maximum number of accounting entries in the interior table to 1,000.

```
<Sysname> system-view
[Sysname] ip count interior-threshold 1000
```

ip count outbound-packets

Syntax **ip count outbound-packets**

undo ip count outbound-packets

View Interface view

Parameter None

Description Use the **ip count outbound-packets** command to count outgoing IP packets on the current interface.

Use the **undo ip count outbound-packets** command to restore the default.

By default, outgoing IP packets on the interface are not counted.

You can execute this command in interface view to count outgoing IP packets, which will be stored in the exterior table or interior table, depending on whether they match the accounting rules.

Example # Count outgoing IP packets on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip count outbound-packets
```

ip count rule

Syntax **ip count rule** *ip-address* { *mask* | *mask-length* }

undo ip count rule {*ip-address* { *mask* | *mask-length* }]

View System view

Parameter *ip-address*: IP address.

mask: Subnet mask.

mask-length: Length of a subnet mask, in the range of 0 to 32.

Description Use the **ip count rule** command to create an IP accounting rule.

Use the **undo ip count rule** command to remove the specified accounting rule. All IP accounting rules will be deleted if no parameter is specified.

Each IP accounting rule consists of an IP address and its mask, namely, a network address, which is the result of ANDing the IP address with its mask. IP packets are sorted as follows:

- If a firewall is configured on an interface and incoming and outgoing IP packets are denied by the firewall, these IP packets are counted in the firewall-denied table.
- If the source or destination IP address of the IP packets passing the interface (in this case, a firewall may be configured or not) matches a network address in the rule, the packets are counted in the interior table. Otherwise, the packets are counted in the exterior table.

Note that:

- You can configure up to 32 rules.
- If no rule is configured, the current packets are not concerned and are all counted in the exterior table.

Example # Create an IP accounting rule.

```
<Sysname> system-view
[Sysname] ip count rule 169.254.10.1 255.255.0.0
```

ip count timeout

Syntax **ip count timeout** *minutes*

undo ip count timeout

View System view

Parameter *minutes*: Aging time in minutes for an accounting entry, in the range of 60 to 10,080.

Description Use the **ip count timeout** command to configure aging time for an IP accounting entry.

Use the **undo ip count timeout** command to restore the default.

By default, the aging time for an accounting entry is 720 minutes, namely, 12 hours.

If an accounting entry is not updated before its aging time expires, the entry is considered expired and then deleted.

Example # Set the aging time for an IP accounting entry to 100 minutes.

```
<Sysname> system-view
[Sysname] ip count timeout 100
```

reset ip count

Syntax **reset ip count** { **all** | **exterior** | **firewall** | **interior** }

View User view

Parameter **all:** Clears all statistics.

firewall: Clears the statistics from the firewall-denied table.

exterior: Clears the statistics from the exterior table.

interior: Clears the statistics from the interior table.

Description Use the **reset ip count** command to clear the statistics of IP packets.

Example # Clear the statistics of all IP packets.

```
<Sysname> reset ip count all
```

59 IP ADDRESSING CONFIGURATION COMMANDS

display ip interface

Syntax **display ip interface** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display ip interface** command to display information about a specified or all Layer 3 interfaces.

Example # Display detailed information about IP for interface Ethernet 1/0.

```
<Sysname> display ip interface ethernet 1/0
Ethernet1/0 current state : DOWN
Line protocol current state : DOWN
Internet Address is 1.1.1.1/8 Primary
Broadcast address : 1.255.255.255
The Maximum Transmit Unit : 1500 bytes
ip fast-forwarding incoming packets state is Disable
ip fast-forwarding outgoing packets state is Disable
input packets : 0, bytes : 0, multicasts : 0
output packets : 0, bytes : 0, multicasts : 0
ARP packet input number:           0
  Request packet:                  0
  Reply packet:                    0
  Unknown packet:                  0
TTL invalid packet number:         0
ICMP packet input number:          0
  Echo reply:                      0
  Unreachable:                     0
  Source quench:                   0
  Routing redirect:                0
  Echo request:                    0
  Router advert:                   0
  Router solicit:                  0
  Time exceed:                     0
  IP header bad:                   0
  Timestamp request:               0
  Timestamp reply:                 0
  Information request:             0
  Information reply:               0
  Netmask request:                 0
  Netmask reply:                   0
```

```
  Unknown type:                       0
DHCP packet deal mode:  global
```

Table 154 Description on fields of the display ip interface command

Field	Description
current state	Current physical state of an interface
Line protocol current state	Current state of the network layer protocol
Internet Address	IP address of an interface followed by: ■ Primary: Identifies a primary IP address, or ■ Sub: Identifies a secondary IP address.
Broadcast address	Broadcast address of the subnet attached to an interface
The Maximum Transmit Unit	Maximum transmission units on an interface
ip fast-forwarding incoming packets state	Enabled/disabled state of fast-forwarding incoming packets on an interface
ip fast-forwarding outgoing packets state	Enabled/disabled state of fast-forwarding outgoing packets on an interface
input packets : 0, bytes : 0, multicasts : 0 output packets : 0, bytes : 0, multicasts : 0	Unicast packets, bytes, and multicast packets received on an interface Unicast packets, bytes, and multicast packets sent on an interface
ARP packet input number: 0 Request packet: 0 Reply packet: 0 Unknown packet: 0	Total number of ARP packets received on an interface, including ■ ARP request packets ■ ARP reply packets ■ Unknown packets
TTL invalid packet number	Number of TTL-invalid packets received on an interface
ICMP packet input number: 0 Echo reply: 0 Unreachable: 0 Source quench: 0 Routing redirect: 0 Echo request: 0 Router advert: 0 Router solicit: 0 Time exceed: 0 IP header bad: 0 Timestamp request: 0 Timestamp reply: 0 Information request: 0 Information reply: 0 Netmask request: 0 Netmask reply: 0 Unknown type: 0	Total number of ICMP packets received on an interface, including the following packets: ■ Echo reply packet ■ Unreachable packets ■ Source quench packets ■ Routing redirect packets ■ Echo request packets ■ Router advertisement packets ■ Router solicitation packets ■ Time exceeded packets ■ IP header bad packets ■ Timestamp request packets ■ Timestamp reply packets ■ Information request packets ■ Information reply packets ■ Netmask request packets ■ Netmask reply packets ■ Unknown type packets

Table 154 Description on fields of the display ip interface command

Field	Description
DHCP packet deal mode	DHCP packet processing mode. This field appears on a DHCP-supporting device and can be one of the following values: ■ global: The DHCP server with the global address pool is enabled on the interface. ■ relay: The DHCP relay agent is enabled on the interface.

display ip interface brief

Syntax **display ip interface brief** [*interface-type* [*interface-number*]]

View Any view

Parameter *interface-type*: Interface type.

interface-number: Interface number.

Description Use the **display ip interface brief** command to display brief information about a specified or all Layer 3 interfaces.

Without the interface type and interface number specified, information about all layer 3 interfaces is displayed; with only the interface type specified, the information about all layer 3 interfaces of the specified type is displayed; with both the interface type and interface number specified, only the information about the specified interface is displayed.

Note that:

If you have configured the time slots of a CE1/PRI or CT1/PRI interface as an ISDN PRI group using the **pri-set** command, then executing the **display ip interface brief** command only displays the time slot used by the control channel (D channel), instead of the ones used by the user channels (B channels). For details about CE1/PRI and CT1/PRI interfaces, refer to "Fundamental CE1/PRI Interface Configuration Commands" on page 201 and "Fundamental CT1/PRI Interface Configuration Commands" on page 213.

Related command: **display ip interface**.

*E1/T1 interfaces are time slotted. Using the pri-set command can bind time slots of an E1/T1 interface into an ISDN PRI group, with each time slot corresponding to a serial interface. To make the displayed output simple and clear, only the time slot of the control channel (D channel) is displayed regardless of whether the **display ip interface brief** command has an interface included or not.*

Example # Display brief information about Ethernet 1/0.

```
<Sysname> display ip interface brief ethernet 1/0
*down: administratively down
(s): spoofing
Interface            Physical        Protocol        IP Address
Ethernet1/0       up              up            192.168.0.1
```

Table 155 Description on fields of the display ip interface brief command

Field	Description
*down	The interface is administratively shut down with the **shutdown** command.
(s)	Spoofing attribute of the interface. It indicates that an interface whose network layer protocol is displayed up may have no link present or the link is set up only on demand.
Interface	Interface name
Physical	Physical state of interface
Protocol	Network layer protocol state of interface
IP Address	IP address of interface (if no IP address is configured, "unassigned" is displayed.)

ip address

Syntax **ip address** *ip-address* { *mask* | *mask-length* } [**sub**]

undo ip address [*ip-address* { *mask* | *mask-length* } [**sub**]]

View Interface view

Parameter *ip-address*: IP address of interface, in dotted decimal notation.

mask: Subnet mask in dotted decimal notation.

mask-length: Subnet mask length, the number of consecutive ones in the mask.

sub: Secondary IP address for the interface.

Description Use the **ip address** command to assign an IP address and mask to the interface.

Use the **undo ip address** command to remove all IP addresses.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } command to remove the primary IP address.

Use the **undo ip address** *ip-address* { *mask* | *mask-length* } **sub** command to remove a secondary IP address.

By default, no IP address is assigned to any interface.

When assigning IP addresses to an interface, consider the following:

- You can assign only one primary IP address to an interface.

- The primary and secondary IP addresses can be located in the same network segment.
- Before removing the primary IP address, remove all secondary IP addresses.
- You can assign a secondary IP address only when the interface is not configured to borrow an IP address through IP unnumbered or obtain one through BOOTP, DHCP, or PPP negotiation.

Related command: **display ip interface**.

Example Assign Ethernet1/0 a primary IP address and a secondary IP address, with the subnet masks both being 255.255.255.0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip address 129.102.0.1 255.255.255.0
[Sysname-Ethernet1/0] ip address 202.38.160.1 255.255.255.0 sub
```

ip address unnumbered

Syntax **ip address unnumbered interface** *interface-type interface-number*

undo ip address unnumbered

View Interface view

Parameter **interface** *interface-type interface-number*: Specifies an interface from which the current interface can borrow an IP address.

Description Use the **ip address unnumbered** command to configure the current interface as IP unnumbered to borrow an IP address from another interface.

Use the **undo ip address unnumbered** command to disable IP unnumbered on the interface.

By default, the interface does not borrow IP addresses from other interfaces.

Example # Configure PPP-encapsulated interface Serial 2/2 to borrow IP address from interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface serial 2/2
[Sysname-Serial2/2] ip address unnumbered interface ethernet 1/0
```

60 IP PERFORMANCE CONFIGURATION COMMANDS

display fib

Syntax **display fib** [| { **begin** | **include** | **exclude** } *string* | **acl** *acl-number* | **ip-prefix** *ip-prefix-name*]

View Any view

Parameter **|** { **begin** | **include** | **exclude** } *string*: Displays FIB information in the buffer related to the specified string according to a regular expression.

- The **begin** keyword specifies to display from the first FIB entry that contains the specified string.
- The **include** keyword specifies to display only the FIB entries that include the specified string.
- The **exclude** keyword specifies to display only the FIB entries that do not include the specified string.
- The *string* argument is a case-sensitive string, containing 1 to 256 characters.

acl *acl-number*: Displays FIB information passing a specified ACL numbered from 2000 to 2999.

ip-prefix *ip-prefix-name*: Displays FIB information passing a specified IP prefix list, a string of 1 to 19 characters.

Description Use the **display fib** command to display FIB forward information. If no parameters are specified, all FIB information will be displayed.

Example # Display all FIB information.

```
<Sysname> display fib
FIB Table:
Total number of Routes : 4
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop     Flag  TimeStamp      Interface    Token
10.2.0.0/16       10.2.1.1     U    t[1150900568]  Eth1/0       invalid
10.2.1.1/32       127.0.0.1    HU   t[1150900568]  InLoop0      invalid
127.0.0.0/8       127.0.0.1    U    t[1150623094]  InLoop0      invalid
127.0.0.1/32      127.0.0.1    HU   t[1150623094]  InLoop0      invalid
```

Table 156 Description on the fields of the display fib command

Field	Description
Total number of Routes	Total number of routes in the FIB table
Destination/Mask	Destination address/length of mask
Nexthop	Address of next hop
Flag	Flags of routes: ■ U"-Usable route ■ G"-Gateway route ■ H"-Host route ■ B"-Blackhole route ■ D"-Dynamic route ■ S"-Static route ■ R"-Refused route ■ L"-Route generated by ARP or ESIS
TimeStamp	Time stamp
Interface	Forward interface
Token	LSP index number

Display FIB information passing ACL 2000

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] display fib acl 2000
Route entry matched by access-list 2000:
Summary counts: 2

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop     Flag  TimeStamp      Interface    Token
10.2.0.0/16       10.2.1.1     U    t[1150900568]  Eth1/0       invalid
10.2.1.1/32       127.0.0.1    HU   t[1150900568]  InLoop0      invalid
```

Display all entries that contain the string "127" and start from the first one.

```
<Sysname> display fib | begin 127
Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop     Flag  TimeStamp      Interface    Token
10.2.1.1/32       127.0.0.1    HU   t[1150900568]  InLoop0      invalid
127.0.0.0/8       127.0.0.1    U    t[1150623094]  InLoop0      invalid
127.0.0.1/32      127.0.0.1    HU   t[1150623094]  InLoop0      invalid
```

Display FIB information passing the IP prefix list abc0

```
<Sysname> system-view
[Sysname] ip ip-prefix abc0 permit 10.2.0.0 16
[Sysname] display fib ip-prefix abc0
Route Entry matched by prefix-list abc0:
Summary count: 1

Flag:
```

```
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop     Flag  TimeStamp      Interface    Token
10.2.0.0/16       10.2.1.1     U    t[1150900568]  Eth1/0       invalid
```

display fib ip-address

Syntax **display fib** *ip-address1* [{ *mask1* | *mask-length1* } [*ip-address2* { *mask2* | *mask-length2* } | **longer**] | **longer**]

View Any view

Parameter *ip-address1, ip-address2*: Destination IP address, in dotted decimal notation. *ip-address1* and *ip-address2* together determine an address range for the FIB entries to be displayed.

mask1, mask2: IP address mask.

mask-length1, mask-length2: Length of IP address mask.

longer: Displays FIB entries that match the specified address/mask and have masks longer than or equal to the mask that a user enters. If no masks are specified, FIB entries that match the natural network address and have the masks longer than or equal to the natural mask will be displayed.

Description Use the **display fib** *ip-address* command to display FIB entries that match the specified destination IP address.

Example # Display the FIB entries that match the natural network of 10.1.0.0 and have the masks longer than or equal to the natural mask.

```
<Sysname> display fib 10.1.0.0 longer
  Route Entry Count: 2

 Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static
  R:Reject   L:Generated by ARP or ESIS

Destination/Mask  Nexthop      Flag   TimeStamp      Interface    Token
10.0.0.0/8        10.1.1.1      U     t[1141140133]  Eth1/0       invalid
10.1.1.1/32       127.0.0.1     HU    t[1141140133]  InLoop0      invalid
```

For description about the above output, refer to Table 156.

display fib statistics

Syntax **display fib statistics**

View Any view

Parameter None

Description Use the **display fib statistics** command to display statistics about the FIB entries.

Example # Display statistics about the FIB entries.

```
<Sysname> display fib statistics
Route Entry Count          : 2
```

Table 157 Description on the fields of the display fib statistics command

Field	Description
Route Entry Count	Number of FIB entries

display icmp statistics

Syntax **display icmp statistics**

View Any view

Parameter None

Description Use the **display icmp statistics** command to display ICMP statistics.

Related command: **display ip interface** and **reset ip statistics**.

Example # Display ICMP statistics.

```
<Sysname> display icmp statistics
  Input: bad formats   0                   bad checksum            0
         echo          5                   destination unreachable 0
         source quench 0                   redirects               0
         echo reply    10                  parameter problem       0
         timestamp     0                   information request     0
         mask requests 0                   mask replies            0
         time exceeded 0
  Output:echo          10                  destination unreachable 0
         source quench 0                   redirects               0
         echo reply    5                   parameter problem       0
         timestamp     0                   information reply       0
         mask requests 0                   mask replies            0
         time exceeded 0
```

Table 158 Description on the fields of the display icmp statistics command

Field	Description
bad formats	Number of input wrong format packets
bad checksum	Number of input wrong checksum packets
echo	Number of input/output echo packets
destination unreachable	Number of input/output destination unreachable packets
source quench	Number of input/output source quench packets
redirects	Number of input/output redirection packets
echo reply	Number of input/output replies

Table 158 Description on the fields of the display icmp statistics command

Field	Description
parameter problem	Number of input/output parameter problem packets
timestamp	Number of input/output time stamp packets
information request	Number of input information request packets
mask requests	Number of input/output mask requests
mask replies	Number of input/output mask replies
information reply	Number of output information reply packets
time exceeded	Number of input/output expiration packets

display ip socket

Syntax **display ip socket** [**socktype** *sock-type*] [*task-id socket-id*]

View Any view

Parameter **socktype** *sock-type*: Displays the socket information of this type. The sock type is in the range 1 to 3, corresponding to TCP, UDP and raw IP respectively.

task-id: Displays the socket information of this task. Task ID is in the range 1 to 100.

socket-id: Displays the information of the socket. Socket ID is in the range 0 to 3072.

Description Use the **display ip socket** command to display socket information.

Example # Display all socket information.

```
<Sysname> display ip socket
SOCK_STREAM:
Task = VTYD(18), socketid = 1, Proto = 6,
LA = 0.0.0.0:23, FA = 0.0.0.0:0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_KEEPALIVE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 2, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.56:1161,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

Task = VTYD(18), socketid = 3, Proto = 6,
LA = 10.153.17.99:23, FA = 10.153.17.82:1121,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_KEEPALIVE SO_OOBINLINE SO_SENDVPNID SO_SETKEEPALIVE,
socket state = SS_ISCONNECTED SS_PRIV SS_ASYNC

SOCK_DGRAM:
Task = IKE(63), socketid = 2, Proto = 17,
LA = 0.0.0.0:500, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_REUSEPORT SO_UDPCHECKSUM,
```

```
socket state = SS_PRIV

Task = RDSO(59), socketid = 1, Proto = 17,
LA = 0.0.0.0:1024, FA = 0.0.0.0:0,
sndbuf = 9216, rcvbuf = 41600, sb_cc = 0, rb_cc = 0,
socket option = SO_UDPCHECKSUM,
socket state = SS_PRIV

SOCK_RAW:
Task = ROUT(68), socketid = 2, Proto = 65,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = ROUT(68), socketid = 1, Proto = 2,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 32767, rcvbuf = 256000, sb_cc = 0, rb_cc = 0,
socket option = SO_SENDVPNID(0),
socket state = SS_PRIV SS_NBIO SS_ASYNC

Task = RSVP(73), socketid = 1, Proto = 46,
LA = 0.0.0.0, FA = 0.0.0.0,
sndbuf = 4194304, rcvbuf = 4194304, sb_cc = 0, rb_cc = 0,
socket option = 0,
socket state = SS_PRIV SS_NBIO SS_ASYNC
```

Table 159 Description on the fields of the display ip socket command

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	raw IP socket
Task	Task number
socketid	Socket ID
Proto	Protocol number of the socket
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	sending buffer size of the socket
rcvbuf	receiving buffer size of the socket
sb_cc	Current data size in the sending buffer (It is available only for TCP that can buffer data)
rb_cc	Data size currently in the receiving buffer
socket option	Socket option
socket state	Socket state

display ip statistics

Syntax **display ip statistics**

View Any view

Parameter None

Description Use the **display ip statistics** command to display statistics of IP packets.

Related command: **display ip interface** and **reset ip statistics**.

Example # Display statistics of IP packets.

```
<Sysname> display ip statistics
  Input:    sum            7120             local             112
            bad protocol   0                bad format        0
            bad checksum   0                bad options       0
  Output:   forwarding     0                local             27
            dropped        0                no route          2
            compress fails 0
  Fragment:input           0                output            0
            dropped        0
            fragmented     0                couldn't fragment 0
  Reassembling:sum         0                timeouts          0
```

Table 160 Description on the fields of the display ip statistics command

Field		Description
Input:	sum	Total number of packets received
	local	Total number of packets with destination being local
	bad protocol	Total number of unknown protocol packets
	bad format	Total number of packets with incorrect format
	bad checksum	Total number of packets with incorrect checksum
	bad options	Total number of packets with incorrect option
Output:	forwarding	Total number of packets forwarded
	local	Total number of packets sent from the local
	dropped	Total number of packets discarded
	no route	Total number of packets for which no route is available
	compress fails	Total number of packets failed to compress
Fragment:	input	Total number of fragments received
	output	Total number of fragments sent
	dropped	Total number of fragments dropped
	fragmented	Total number of packets successfully fragmented
	couldn't fragment	Total number of packets that failed to be fragmented
Reassembling	sum	Total number of packets reassembled
	timeouts	Total number of reassembly timeout fragments

display tcp statistics

Syntax **display tcp statistics**

View Any view

Parameter None

Description Use the **display tcp statistics** command to display statistics of TCP traffic.

Related command: **display tcp status** and **reset tcp statistics**.

Example # Display statistics of TCP traffic.

```
<Sysname> display tcp statistics
Received packets:
Total: 753
packets in sequence: 412 (11032 bytes)
window probe packets: 0, window update packets: 0
checksum error: 0, offset error: 0, short error: 0

duplicate packets: 4 (88 bytes), partially duplicate packets: 5 (7 bytes)
out-of-order packets: 0 (0 bytes)
packets of data after window: 0 (0 bytes)
packets received after close: 0

ACK packets: 481 (8776 bytes)
duplicate ACK packets: 7, too much ACK packets: 0

Sent packets:
Total: 665
urgent packets: 0
control packets: 5 (including 1 RST)
window probe packets: 0, window update packets: 2

data packets: 618 (8770 bytes) data packets retransmitted: 0 (0 bytes)
ACK-only packets: 40 (28 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, Keepalive timeout, so connections
disconnected : 0
Initiated connections: 0, accepted connections: 0, established connections:0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
Packets dropped with MD5 authentication: 0
Packets permitted with MD5 authentication: 0
```

Table 161 Description on the fields of the display tcp statistics command

Field		Description
Received packets:	Total	Total number of packets received
	packets in sequence	Number of packets arriving in sequence
	window probe packets	Number of window probe packets received
	window update packets	Number of window update packets received
	checksum error	Number of checksum error packets received
	offset error	Number of offset error packets received
	short error	Number of received packets with length being too small
	duplicate packets	Number of completely duplicate packets received
	partially duplicate packets	Number of partially duplicate packets received
	out-of-order packets	Number of out-of-order packets received
	packets of data after window	Number of packets outside the receiving window
	packets received after close	Number of packets that arrived after connection is closed
	ACK packets	Number of ACK packets received
	duplicate ACK packets	Number of duplicate ACK packets received
	too much ACK packets	Number of ACK packets for data unsent
Sent packets:	Total	Total number of packets sent
	urgent packets	Number of urgent packets sent
	control packets	Number of control packets sent
	window probe packets	Number of window probe packets sent; in the brackets are resent packets
	window update packets	Number of window update packets sent
	data packets	Number of data packets sent
	data packets retransmitted	Number of data packets retransmitted
	ACK-only packets	Number of ACK packets sent; in brackets are delayed ACK packets
Retransmitted timeout		Number of retransmission timer timeouts
connections dropped in retransmitted timeout		Number of connections broken due to retransmission timeouts
Keepalive timeout		Number of keepalive timer timeouts
keepalive probe		Number of keepalive probe packets sent
Keepalive timeout, so connections disconnected		Number of connections broken due to timeout of the keepalive timer
Initiated connections		Number of connections initiated
accepted connections		Number of connections accepted
established connections		Number of connections established
Closed connections		Number of connections closed; in brackets are connections closed accidentally (before receiving SYN from the peer) and connections closed initiatively (after receiving SYN from the peer)

Table 161 Description on the fields of the display tcp statistics command

Field	Description
Packets dropped with MD5 authentication	Number of packets dropped with MD5 authentication
Packets permitted with MD5 authentication	Number of packets permitted with MD5 authentication

display tcp status

Syntax **display tcp status**

View Any view

Parameter None

Description Use the **display tcp status** command to display status of all TCP connection for monitoring TCP connections.

Example # Display status of all TCP connections

```
<Sysname> display tcp status
*: TCP MD5 Connection
TCPCB         Local Add:port       Foreign Add:port     State
03e37dc4      0.0.0.0:4001         0.0.0.0:0            Listening
04217174      100.0.0.204:23       100.0.0.253:65508    Established
```

Table 162 Description on the fields of the display tcp status command

Field	Description
*	If the status information of a TCP connection contains *, the TCP adopts the MD5 algorithm for authentication.
TCPCB	TCP control block
Local Add:port	Local IP address and port number
Foreign Add:port	Remote IP address and port number
State	State of the TCP connection

display udp statistics

Syntax **display udp statistics**

View Any view

Parameter None

Description Use the display udp statistics command to display statistics of UDP packets.

Related command: **reset udp statistics**.

Example # Display statistics of UDP packets.

```
<Sysname> display udp statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

Table 163 Description on the fields of the display udp statistics command

Field		Description
Received packets:	Total	Total number of UDP packets received
	checksum error	Total number of packets with incorrect checksum
	shorter than header	Number of packets with data shorter than head
	data length larger than packet	Number of packets with data longer than packet
	unicast(no socket on port)	Number of unicast packets with no socket on port
	broadcast/multicast(no socket on port)	Number of broadcast/multicast packets without socket on port
	not delivered, input socket full	Number of packets not delivered to upper layer due to socket buffer being full
	input packets missing pcb cache	Number of packets without matching PCB cache
Sent packets:	Total	Total number of UDP packets sent

ip forward-broadcast

Syntax **ip forward-broadcast** [**acl** *acl-number*]

undo ip forward-broadcast

View Interface view

Parameter **acl** *acl-number*: Number of an ACL from 2000 to 3999. From 2000 to 2999 are numbers for basic ACLs, and from 3000 to 3999 are numbers for advanced ACLs. Only directed broadcasts permitted by the ACL can be forwarded.

Description Use the **ip forward-broadcast** command to enable the interface to forward directed broadcasts.

Use the **undo ip forward-broadcast** command to disable an interface from forwarding directed broadcasts.

By default, an interface is disabled from forwarding directed broadcasts.

Example # Allow Ethernet 1/0 to forward directed broadcasts permitted by ACL 2001.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip forward-broadcast acl 2001
```

ip redirects enable

Syntax **ip redirects enable**

undo ip redirects

View System view

Parameter None

Description Use the **ip redirects enable** command to enable sending ICMP redirect packets.

Use the **undo ip redirects** command to disable sending ICMP redirect packets.

This feature is enabled by default.

Example # Disable sending ICMP redirection packets.

```
<Sysname> system-view
[Sysname] undo ip redirects
```

ip ttl-expires enable

Syntax **ip ttl-expires enable**

undo ip ttl-expires

View System view

Parameter None

Description Use the **ip ttl-expires enable** command to enable the sending of ICMP timeout packets.

Use the **undo ip ttl-expires** command to disable sending ICMP timeout packets.

Sending ICMP timeout packets is enabled by default.

If the feature is disabled, the device will not send TTL timeout ICMP packets, but still send "reassembly timeout" ICMP packets.

Example # Disable sending ICMP timeout packets.

```
<Sysname> system-view
[Sysname] undo ip ttl-expires
```

ip unreachables enable

Syntax **ip unreachables enable**

undo ip unreachables

View System view

Parameter None

Description Use the **ip unreachables enable** command to enable the sending of ICMP destination unreachable packets.

Use the **undo ip unreachables** command to disable sending ICMP destination unreachable packets.

Sending ICMP destination unreachable packets is enabled by default.

If the feature is disabled, the device will not send network unreachable and source route failure ICMP packets, but still send other destination unreachable ICMP packets.

Example # Disable sending ICMP destination unreachable packets.

```
<Sysname> system-view
[Sysname] undo ip unreachables
```

reset ip statistics

Syntax **reset ip statistics**

View User view

Parameter None

Description Use the **reset ip statistics** command to clear statistics of IP packets.

Related command: **display ip interface** and **display ip statistics**.

Example # Clear statistics of IP packets.

```
<Sysname> reset ip statistics
```

reset tcp statistics

Syntax **reset tcp statistics**

View User view

Parameter None

Description Use the **reset tcp statistics** command to clear statistics of TCP traffic.

Related command: **display tcp statistics**.

Example # Display statistics of TCP traffic.

```
<Sysname> reset tcp statistics
```

reset udp statistics

Syntax **reset udp statistics**

View User view

Parameter None

Description Use the **reset udp statistics** command to clear statistics of UDP traffic.

Example # Display statistics of UDP traffic.

```
<Sysname> reset udp statistics
```

tcp anti-naptha enable

Syntax **tcp anti-naptha enable**

undo tcp anti-naptha enable

View System view

Parameter None

Description Use the **tcp anti-naptha enable** command to enable the protection against Naptha attack.

Use the **undo tcp anti-naptha enable** command to disable the protection against Naptha attack.

By default, the protection against Naptha attack is disabled.

Note that the configurations of the **tcp state** and **tcp timer check-state** command will be deleted after the protection against Naptha attack is disabled.

The support for this command varies with devices.

Example # Enable the protection against Naptha attack.

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
```

tcp mss

Syntax **tcp mss** *value*

undo tcp mss

View Interface view

Parameter *value*: Maximum size of a packet in bytes, ranging from 128 to 2,048.

Description Use the **tcp mss** command to configure the maximum size of TCP packets.

Use the **undo tcp mss** command to restore the default.

By default, the maximum size of a TCP packet is 1460 bytes.

As the default MTU on an interface is 1500 bytes, and there are link layer cost and IP packet head, so the recommended maximum size of TCP packets is about 1200 bytes.

Example # Set the maximum size of TCP packets to 300 bytes on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] tcp mss 300
```

tcp state

Syntax **tcp state** { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** | **syn-received** } **connection-number** *number*

undo tcp state { **closing** | **established** | **fin-wait-1** | **fin-wait-2** | **last-ack** | **syn-received** } **connection-number**

View System view

Parameter **closing**: CLOSING state of a TCP connection.

established: ESTABLISHED state of a TCP connection.

fin-wait-1: FIN_WAIT_1 state of a TCP connection.

fin-wait-2: FIN_WAIT_2 state of a TCP connection.

last-ack: LAST_ACK state of a TCP connection.

syn-received: SYN_RECEIVED state of a TCP connection.

connected-number *number*: Maximum number of TCP connections in a certain state. The argument *number* is in the range of 0 to 500.

Description Use the **tcp state** command to configure the maximum number of TCP connections in a state. When this number is exceeded, the aging of TCP connections in this state will be accelerated.

Use the **undo tcp state** command to restore the default.

By default, the maximum number of TCP connections in each state is 5.

Note the following points:

- You need to enable the protection against Naptha attack before executing this command. Otherwise, an error will be prompted.
- You can respectively configure the maximum number of TCP connections in each state.
- If the maximum number of TCP connections in a state is 0, the aging of TCP connections in this state will not be accelerated.

Related command: **tcp anti-naptha enable**.

This support for this command varies with devices.

Example # Set the maximum number of TCP connections in the ESTABLISHED state to 100.

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
[Sysname] tcp state established connection-number 100
```

tcp syn-cookie enable

Syntax **tcp syn-cookie enable**

undo tcp syn-cookie enable

View System view

Parameter None

Description Use the **tcp syn-cookie enable** command to enable the SYN Cookie feature to protect the device against SYN Flood attacks.

Use the **undo tcp syn-cookie enable** command to disable the SYN Cookie feature.

By default, the SYN Cookie feature is disabled.

The support for this command varies with devices.

Example # Enable the SYN Cookie feature.

```
<Sysname> system-view
[Sysname] tcp syn-cookie enable
```

tcp timer check-state

Syntax **tcp timer check-state** *time-value*

undo tcp timer check-state

View System view

Parameter *time-value*: TCP connection state check interval in seconds, in the range of 1 to 60.

Description Use the **tcp timer check-state** command to configure the TCP connection state check interval.

Use the **undo tcp timer check-state** command to restore the default.

By default, the TCP connection state check interval is 30 seconds.

The device periodically checks the number of TCP connections in each state. If it detects that the number of TCP connections in a state exceeds the maximum number, it will accelerate the aging of TCP connections in such a state.

Note that you need to enable the protection against Naptha attack before executing this command. Otherwise, an error will be prompted.

Related command: **tcp anti-naptha enable**.

The support for this command varies with devices.

Example # Set the TCP connection state check interval to 40 seconds.

```
<Sysname> system-view
[Sysname] tcp anti-naptha enable
[Sysname] tcp timer check-state 40
```

tcp timer fin-timeout

Syntax **tcp timer fin-timeout** *time-value*

undo tcp timer fin-timeout

View System view

Parameter *time-value*: Length of the TCP finwait timer in seconds, ranging from 76 to 3,600.

Description Use the **tcp timer fin-timeout** command to configure the length of the TCP finwait timer.

Use the **undo tcp timer fin-timeout** command to restore the default.

By default, the length of the TCP finwait timer is 675 seconds.

Note that the actual length of the finwait timer is determined by the following formula:

Actual length of the finwait timer = (Configured length of the finwait timer - 75) + configured length of the synwait timer

Related command: **tcp timer syn-timeout** and **tcp window**.

Example # Set the length of the TCP finwait timer to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp timer fin-timeout 800
```

tcp timer syn-timeout

Syntax **tcp timer syn-timeout** *time-value*

undo tcp timer syn-timeout

View System view

Parameter *time-value*: Length of the TCP finwait timer in seconds, ranging from 2 to 600.

Description Use the **tcp timer syn-timeout** command to configure the length of the TCP synwait timer.

Use the **undo tcp timer syn-timeout** command to restore the default.

By default, the length of the TCP synwait timer is 75 seconds.

Related command: **tcp timer fin-timeout** and **tcp window**.

Example # Set the length of the TCP synwait timer to 80 seconds.

```
<Sysname> system-view
[Sysname] tcp timer syn-timeout 80
```

tcp window

Syntax **tcp window** *window-size*

undo tcp window

View System view

Parameter *window-size*: Receiving/sending buffer size of TCP connection in KB, ranging from 1 to 32.

Description Use the **tcp window** command to configure the receiving/sending buffer size of TCP connection.

Use the **undo tcp window** command to restore the default.

The TCP receiving/sending buffer is 8 KB by default.

Related command: **tcp timer fin-timeout** and **tcp timer syn-timeout**.

Example # Configure the receiving/sending buffer of TCP connection as 3 KB.

```
<Sysname> system-view
[Sysname] tcp window 3
```

61 IP UNICAST POLICY ROUTING CONFIGURATION COMMANDS

apply default output-interface

Syntax **apply default output-interface** *interface-type interface-number* [**track** *track-entry-number*] [*interface-type interface-number* [**track** *track-entry-number*]]

undo apply default output-interface [*interface-type interface-number* [*interface-type interface-number*]]

View policy-based-route view

Parameters *interface-type interface-number*: Specifies an interface.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* is in the range 1 to 1024.

Description Use the **apply default output-interface** command to set the default outgoing interface for matched packets.

Use the **undo apply default output-interface** command to remove the configuration.

Using this command can set two outgoing interfaces at most for load-sharing.

Related commands: **apply ip-precedence**, **apply ip-address next-hop**, **apply output-interface**, and **apply ip-address default next-hop**.

Examples # Set the default outgoing interface for matched packets to Serial2/0.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] apply default output-interface serial 2
/0 track 1
```

apply ip-address default next-hop

Syntax **apply ip-address default next-hop** *ip-address* [**track** *track-entry-number*] [*ip-address* [**track** *track-entry-number*]]

undo apply ip-address default next-hop [*ip-address* [*ip-address*]]

View policy-based-route view

Parameters *ip-address*: IP address of the default next hop.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* is in the range 1 to 1024.

Description Use the **apply ip-address default next-hop** command to set the default next hop for matched packets.

Use the **undo apply ip-address default next-hop** command to remove the configuration.

At most two default next hops can be specified in one command line.

The next hop interface must be a point-to-point (P2P) interface rather than a broadcast interface.

Related commands: **apply ip-precedence**, **apply output-interface**, **apply default output-interface**, and **apply ip-address next-hop**.

Examples # Set the default next hop to 1.1.1.1 for matched packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] apply ip-address default next-hop 1.1.1
.1 track 1
```

apply ip-address next-hop

Syntax **apply ip-address next-hop** *ip-address* [**track** *track-entry-number*] [*ip-address* [**track** *track-entry-number*]]

undo apply ip-address next-hop [*ip-address* [*ip-address*]]

View policy-based-route view

Parameters *ip-address*: IP address of the next hop.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* is in the range 1 to 1024.

Description Use the **apply ip-address next-hop** command to set a next hop for matched packets.

Use the **undo apply ip-address next-hop** command to remove the configuration.

You can specify up to two next hops in one command line for load-sharing.

Related commands: **apply ip-precedence**, **apply output-interface**, **apply default output-interface**, and **apply ip-address default next-hop**.

Examples # Set the next hop to 1.1.1.1 for matched packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] apply ip-address next-hop 1.1.1.1 track 1
```

apply ip-precedence

Syntax **apply ip-precedence** { *type* | *value* }

undo apply ip-precedence

View policy-based-route view

Parameters *type:* Specifies the precedence type of IP packets.

value: Specifies a precedence value. There are eight precedences (0 to 7) for an IP packet, each corresponding to a keyword. The precedences are listed in the following table:

Table 164 IP precedences and the corresponding keywords

Precedence	Keyword
0	routine
1	priority
2	immediate
3	flash
4	flash-override
5	critical
6	internet
7	network

Description Use the **apply ip-precedence** command to set a precedence for matched packets.

Use the **undo apply ip-precedence** command to remove the setting.

Related commands: **apply output-interface**, **apply ip-address next-hop**, **apply default output-interface**, and **apply ip-address default next-hop**.

Examples # Set the precedence to 5 (critical) for matched packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] apply ip-precedence critical
```

apply output-interface

Syntax **apply output-interface** *interface-type interface-number* [**track** *track-entry-number*] [*interface-type interface-number* [**track** *track-entry-number*]]

undo apply output-interface [*interface-type interface-number* [*interface-type interface-number*]]

View policy-based-route view

Parameters *interface-type interface-number*: Specifies an interface.

track *track-entry-number*: Specifies a track entry. The *track-entry-number* is in the range 1 to 1024.

Description Use the **apply output-interface** command to set the outgoing interface(s) for matched packets.

Use the **undo apply output-interface** command to remove the configuration.

This command is used to specify interfaces (two interfaces at most) to send the matched IP packets.

Note that:

- Two outgoing interfaces at most can be specified for matched IP packets.
- For non-P2P interfaces (broadcast and NBMA interfaces) such as Ethernet interface, multiple next hops are available, and thus packets may not be forwarded successfully.

Non-broadcast multi-access (NBMA) network adopts the unicast mode to send packets.

Related commands: **apply ip-precedence**, **apply ip-address next-hop**, **apply default output-interface**, and **apply ip-address default next-hop**.

Examples # Specify Serial2/0 as the outgoing interface for matched IP packets.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] apply output-interface serial 2/0 track 1
```

display ip policy-based-route

Syntax **display ip policy-based-route**

View Any view

Parameters None

Description Use the **display ip policy-based-route** command to display all system and interface policy routing information.

Examples # Display all system and interface policy routing information.

```
<Sysname> display ip policy-based-route
Policy Name             interface
pr02                        local
pr02                        Virtual-Template0
pr01                        Ethernet 1/0
```

Table 165 Description on fields of the display ip policy-based-route command

Field	Description
local	System policy routing.
pr02	Name of the policy.
Virtual-Template0	Indicates that the policy named pr02 is applied to interface Virtual-template0.
Ethernet1/0	Indicates that the policy named pr01 is applied to interface Ethernet1/0.

display ip policy-based-route setup

Syntax **display ip policy-based-route setup** { *policy-name* | **interface** *interface-type interface-number* | **local** }

View Any view

Parameters *policy-name*: Displays policy routing information about the specified policy. A policy name is a string of 1 to 19 characters.

interface *interface-type interface-number*: Displays the configuration of policy routing enabled on the interface specified by the argument *interface-type interface-number*.

local: Displays the configuration of enabled system policy routing.

Description Use the **display ip policy-based-route setup** command to display the configuration of enabled policy routing.

Examples # Display the configuration of policy routing enabled on interface Ethernet1/0.

```
<Sysname> display ip policy-based-route setup interface ethernet 1/0
Interface Ethernet1/0 policy based routing configuration information:
 policy-based-route pr01
  permit node 1
    if-match acl 3101
    apply output-interface Ethernet1/0
```

Table 166 Description on fields of the display ip policy-based-route setup command

Field	Description
Interface Ethernet1/0 policy based routing configuration information	Configuration information of policy routing enabled on interface Ethernet1/0

Table 166 Description on fields of the display ip policy-based-route setup command

Field	Description
policy-based-route pr01	The referenced policy name is pr01.
permit node 1	The match mode is **permit** and the policy consists of only node 1.
if-match acl 3101	Packets satisfying ACL 3101 are matched.
apply output-interface Ethernet1/0	The outgoing interface of matched packets is Ethernet1/0.

display ip policy-based-route statistics

Syntax **display ip policy-based-route statistics** { **interface** *interface-type interface-number* | **local** }

View Any view

Parameters **interface** *interface-type interface-number*: Displays statistics of interface policy routing enabled on the interface specified by the argument *interface-type interface-number*.

local: Displays statistics of enabled system policy routing.

Description Use the **display ip policy-based-route statistics** command to display policy routing statistics.

Examples # Display statistics of interface policy routing enabled on interface Ethernet1/0.

```
<Sysname> display ip policy-based-route statistic interface ethernet1/0
Interface Ethernet1/0 policy based routing statistics information:
 policy-based-route: aaa
   permit node 5
     apply output-interface ethernet 1/0
       Denied: 0,
       Forwarded: 0
 Total denied: 0, forwarded: 0
```

Table 167 Description on fields of display ip policy-based-route statistic command

Field	Description
Interface Ethernet1/0 policy based routing statistics information	Statistics of policy routing enabled on interface Ethernet1/0.
policy-based-route: aaa	The policy name is aaa.
permit node 5	The match mode of node 5 is permit.
apply output-interface ethernet 1/0	The outgoing interface of matched packets is Ethernet1/0.
Denied: 0, Forwarded: 0	Unsuccessfully/successfully forwarded packets that match node 5
Total denied: 0, forwarded: 0	Unsuccessfully/successfully forwarded packets that match all nodes of policy aaa

display policy-based-route

Syntax **display policy-based-route** [*policy-name*]

View Any view

Parameters *policy-name*: Policy name, a string of 1 to 19 characters.

Description Use the **display policy-based-route** command to display the configured policy routing information.

Examples # Display the configured policy routing information.

```
<Sysname> display policy-based-route
policy-based-route : aaa
  Node  1  permit :
    apply output-interface Vlan-interface2
```

Table 168 Description on the fields of the display policy-based-route command

Field	Description
policy-based-route : aaa	The policy name is **aaa**.
Node 1 permit :	The match mode of node 1 is permit.
apply output-interface Vlan-interface2	The outgoing interface of matched packets is Ethernet1/0.

if-match acl

Syntax **if-match acl** *acl-number*

undo if-match acl

View policy-based-route view

Parameters *acl-number*: ACL number, in the range of 2000 to 3999. The number of a basic ACL ranges from 2000 to 2999 and that of an advanced ACL ranges from 3000 to 3999.

Description Use the **if-match acl** command to define an ACL match rule.

Use the **undo if-match acl** command to remove the ACL match rule.

Related commands: **if-match packet-length**.

Examples # Permit the packets satisfying ACL 2010.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] if-match acl 2010
```

if-match packet-length

Syntax **if-match packet-length** *min-len max-len*

undo if-match packet-length

View policy-based-route view

Parameters *min-len*: Minimum IP packet length in bytes, in the range of 0 to 65535.

max-len: Maximum IP packet length in bytes, in the range of 1 to 65535. *max-len* must be no less than *min-len*.

Description Use the **if-match packet-length** command to define a packet length match rule.

Use the **undo if-match packet-length** command to remove the match rule.

Related commands: **if-match acl**.

Examples # Permit the packets with a length from 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] policy-based-route aa permit node 11
[Sysname-policy-based-route] if-match packet-length 100 200
```

ip local policy-based-route

Syntax **ip local policy-based-route** *policy-name*

undo ip local policy-based-route *policy-name*

View System view

Parameters *policy-name*: Policy name, which uniquely identifies a policy-based-route. It is a string of 1 to 19 characters.

Description Use the **ip local policy-based-route** command to enable system policy routing and reference a policy.

Use the **undo ip local policy-based-route** command to disable system policy routing.

System policy routing is disabled by default.

Note that:

- You can only reference one policy when enabling system policy routing.

- System policy routing is used to route packets generated locally. Unless otherwise required, you are not recommended to enable system policy routing.

Related commands: **policy-based-route**.

Examples # Enable system policy routing and reference policy aaa.

```
<Sysname> system-view
[Sysname] ip local policy-based-route aaa
```

ip policy-based-route

Syntax **ip policy-based-route** *policy-name*

undo ip policy-based-route *policy-name*

View Interface view

Parameters *policy-name*: Policy name, a string of 1 to 19 characters.

Description Use the **ip policy-based-route** command to enable policy routing and reference a policy on the interface.

Use the **undo ip policy-based-route** command to disable interface policy routing.

Interface policy routing is disabled by default.

Note that:

- You can only reference one policy when enabling policy routing on an interface.
- The referenced policy filters incoming packets on the interface.

Related commands: **ip local policy-based-route**.

Examples # Enable policy routing and reference policy aaa on interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip policy-based-route aaa
```

policy-based-route

Syntax **policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*

undo policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

View System view

Parameters *policy-name*: Policy name, a string of 1 to 19 characters.

deny: Specifies the match mode of the policy node as **deny**. When a packet satisfies all rules defined by the **if-match** clauses, the packet will be refused by the node and will not go to match the next policy node.

permit: Specifies the match mode of the policy node as **permit**. If a packet satisfies all the rules defined by the **if-match** clauses, the **apply** clauses are executed. If not, the packet will go to match the next policy node.

node *node-number*: Number of a policy node, in the range of 0 to 65535. The node with a smaller *node-number* is matched first.

Description Use the **policy-based-route** command to define a policy or policy node and enter policy view.

Use the **undo policy-based-route** command to remove a policy or policy node.

No policy or policy node is defined by default.

The default match mode of a policy node is **permit**.

A policy consists of several nodes, and a node consists of **if-match** clauses and **apply** clauses. The **if-match** clauses define the match rules for the node and the **apply** clauses define the actions that should be taken for matched packets. There is an AND relationship between the **if-match** clauses of a node. That is to say, a packet must satisfy all matching rules specified by all **if match** clauses for the node before the action specified by the **apply** clause is taken.

There is an OR relationship between nodes of the policy. That is, if a packet matches a node, it satisfies the policy.

Related commands: **if-match acl** and **if-match packet-length**.

Examples # Configure a policy named policy1, set the match mode of node 10 to **permit**, and enter policy routing view.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-policy-based-route]
```

reset policy-based-route statistics

Syntax **reset policy-based-route statistics** [*policy-name*]

View User view

Parameters *policy-name*: Policy name, a string of 1 to 19 characters.

Description Use the **reset policy-based-route statistics** command to clear the statistics of policy routing based on a specified policy.

If no policy name is specified, this command clears all the policy routing statistics.

Examples # Clear all the policy routing statistics.

```
<Sysname> reset policy-based-route statistics
```

62 UDP HELPER CONFIGURATION COMMANDS

display udp-helper server

Syntax **display udp-helper server** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Displays information of forwarded UDP packets on the specified interface.

Description Use the **display udp-helper server** command to display the information of forwarded UDP packets on the specified interface or all interfaces.

If *interface-type interface-number* is not specified, this command displays the information of forwarded UDP packets on all interfaces.

Example # Display the information of forwarded UDP packets on the interface Ethernet1/0.

```
<Sysname> display udp-helper server interface ethernet 1/0
Interface name      Server address      Packets sent
Ethernet1/0         192.1.1.2           0
```

The information above shows that the IP address of the destination server corresponding to the interface Ethernet 1/0 is 192.1.1.2, and that no packets are forwarded to the destination server.

reset udp-helper packet

Syntax **reset udp-helper packet**

View User view

Parameter None

Description Use the **reset udp-helper packet** command to clear the statistics of UDP packets forwarded.

Related command: **display udp-helper server**.

Example # Clear the statistics of the forwarded UDP packets.

```
<Sysname> reset udp-helper packet
```

udp-helper enable

Syntax **udp-helper enable**

undo udp-helper enable

View System view

Parameter None

Description Use the **udp-helper enable** command to enable UDP Helper.

Use the **undo udp-helper enable** command to disable UDP Helper.

By default, UDP Helper is disabled.

Example # Enable UDP Helper

```
<Sysname> system-view
[Sysname] udp-helper enable
```

udp-helper port

Syntax **udp-helper port** { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

undo udp-helper port { *port-number* | **dns** | **netbios-ds** | **netbios-ns** | **tacacs** | **tftp** | **time** }

View System view

Parameter *port-number*: UDP port number with which packets need to be forwarded, in the range of 1 to 65535 (except 67 and 68).

dns: Forwards DNS data packets. The corresponding UDP port number is 53.

netbios-ds: Forwards NetBIOS data packets. The corresponding UDP port number is 138.

netbios-ns: Forwards NetBIOS name service data packets. The corresponding UDP port number is 137.

tacacs: Forwards terminal access controller access control system (TACACS) data packets. The corresponding UDP port number is 49.

tftp: Forwards TFTP data packets. The corresponding UDP port number is 69.

time: Forwards time service data packets. The corresponding UDP port number is 37.

Description Use the **udp-helper port** command to enable the forwarding of packets with the specified UDP port number.

Use the **undo udp-helper port** command to remove the configured UDP port numbers.

By default, the UDP Helper enabled device forwards broadcast packets with any of the six destination port numbers 69, 53, 37, 137, 138 and 49. The configured UDP port numbers (including the default UDP port numbers) will all be removed if UDP Helper is disabled.

Example # Forward broadcast packets with the UDP destination port number 100.

```
<Sysname> system-view
[Sysname] udp-helper port 100
```

udp-helper server

Syntax **udp-helper server** *ip-address*

undo udp-helper server [*ip-address*]

View Interface view

Parameter *ip-address*: IP address of the destination server, in dotted decimal notation.

Description Use the **udp-helper server** command to specify the destination server which UDP packets to be forwarded to.

Use the **undo udp-helper server** command to remove the destination server.

No destination server is configured by default.

Currently, you can configure up to 20 destination servers on an interface.

Note that you will remove all the destination servers under the interface if you carry out the **undo udp-helper server** command without the *ip-address* argument.

Related command: **display udp-helper server**.

Example # Specify the IP address of the destination server as 192.1.1.2 on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] udp-helper server 192.1.1.2
```

63 URPF CONFIGURATION COMMANDS

ip urpf

Syntax **ip urpf** { **loose** | **strict** } [**allow-default-route**] [**acl** *acl-number*]

undo ip urpf

View Interface view

Parameter **loose**: Specifies the loose URPF check.

strict: Specifies the strict URPF check.

allow-default-route: Allows special treatment to default route.

acl-number: ACL number, in the range of 2000 to 3999.

- For a basic ACL, the value ranges from 2000 to 2999.
- For an advanced ACL, the value ranges from 3000 to 3999.

Description Use the **ip urpf** command to enable URPF check on the interface.

Use the **undo ip urpf** command to disable this function.

By default, URPF check is disabled.

Example # Enable strict URPF check on interface Ethernet 1/0, allowing special treatment to default route, and referencing ACL 2999.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip urpf strict allow-default-route acl 2999
```

Enable loose URPF check on interface Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ip urpf loose
```

64 FAST FORWARDING COMMANDS

display ip fast-forwarding cache

Syntax **display ip fast-forwarding cache**

View Any view

Parameter None

Description Use the **display ip fast-forwarding cache** command to display the information in the fast forwarding cache.

Example # Display the information in the fast forwarding cache.

```
<Sysname> display ip fast-forwarding cache
Fast-Forwarding cache:  total 3 items
Index  SIP            SPort    DIP       DPort Pro Input_If   Output_If   Flg
412 :0 7.0.0.13       68    8.0.0.1      67    17  Eth1/0   Eth1/1       7
484 :0 8.0.0.1        67    7.0.0.13     68    17  Eth1/1   Eth1/0       7
819 :0 8.0.0.1        8     7.0.0.13     0     1   Eth1/2   Eth1/0       7
```

Table 169 Description on the fields of the display ip fast-forwarding cache command

Field	Description
Index	Unique entry index
SIP	Source IP address
SPort	Source port number
DIP	Destination IP address
DPort	Destination port number
Pro	Protocol number
Input_If	Input interface number
Output_If	Output interface number
Flg	Internal tag, mainly for marking internal operation information such as fragmentation

ip fast-forwarding

Syntax **ip fast-forwarding** [**inbound** | **outbound**]

undo ip fast-forwarding [**inbound** | **outbound**]

View Interface view

Parameter **inbound**: Enables or disables fast forwarding only in the inbound direction.

outbound: Enables or disables fast forwarding only in the outbound direction.

If no parameter is specified, fast forwarding is enabled or disabled in both the inbound and outbound directions.

Description Use the **ip fast-forwarding** command to enable fast forwarding in the inbound and/or outbound direction(s).

Use the **undo ip fast-forwarding** command to disable fast forwarding in the inbound and/or outbound direction(s).

By default, fast forwarding is enabled in both the inbound and outbound directions.

Fast forwarding applies to high speed link interfaces (such as Ethernet and Frame Relay interfaces) rather than low speed link interfaces.

Fast forwarding is supported on high-speed link interfaces (including Ethernet, synchronous PPP, Frame Relay and HDLC interfaces) with firewall, NAT, or GRE configured. Fast forwarding is also supported on PPP MP links and IPHC compression or VJ compression enabled PPP links.

CAUTION:

- *In the case of load balancing using fast forwarding, fast forwarding must be disabled in the corresponding direction of the interface.*
- *The interface on which fast forwarding is enabled stops sending ICMP Redirect messages.*
- *After fast forwarding is enabled on an interface, no IP packet debugging information will be displayed for the interface, that is, the **debugging ip packet** command does not work.*
- *To implement fast forwarding of data flow, you need to enable fast forwarding in the inbound direction of the receive interface and in the outbound direction of the send interface.*
- *When a routing interface is different from its physical interface on links such as MP link or PPPoE links, whether fast forwarding is enabled or not on the physical interface does not affect fast forwarding on the routing interface.*

Example # Enable fast forwarding in the inbound direction of the Ethernet 1/0 interface.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip fast-forwarding inbound
```

Disable fast forwarding in the inbound direction of the Ethernet 1/1 interface.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] undo ip fast-forwarding
```

reset ip fast-forwarding cache

Syntax **reset ip fast-forwarding cache**

View User view

Parameter None

Description Use the **reset ip fast-forwarding cache** command to clear the information in the fast forwarding cache.

Example # Clear the information in the fast forwarding cache.

```
<Sysname> reset ip fast-forwarding cache
```

65 IPv6 Basics Configuration Commands

display dns ipv6 dynamic-host

Syntax **display dns ipv6 dynamic-host**

View Any view

Parameter None

Description Use the **display dns ipv6 dynamic-host** command to display IPv6 dynamic domain name cache information.

Example # Display IPv6 dynamic domain name cache information.

```
<Sysname> display dns ipv6 dynamic-host
No.     Host               IPv6 Address      TTL
1       aaa                 2001::2           6
```

Table 170 Description on fields of the display dns ipv6 dynamic-host command

Field	Description
No	Sequence number
Host	Host name
IPv6 address	IPv6 address of the host
TTL	Time an entry can be cached in seconds

*For a domain name displayed with the **display dns ipv6 dynamic-host** command, no more than 21 characters can be displayed. If the domain name exceeds the maximum length, the first 21 characters will be displayed.*

display dns ipv6 server

Syntax **display dns ipv6 server** [**dynamic**]

View Any view

Parameter **dynamic**: Displays the information of IPv6 DNS servers acquired dynamically through DHCP or other protocols.

Description Use the **display dns ipv6 server** command to display IPv6 DNS server information.

Example # Display IPv6 DNS server information.

```
<Sysname> display dns ipv6 server
 Type:
  D:Dynamic    S:Static

DNS Server  Type  IPv6 Address                                (Interface Name)
     1        S      1::1
     2        S      FE80:1111:2222:3333:4444:5555:6666:7777  Vlan2
```

Table 171 Description on the fields of the display dns ipv6 server command

Field	Description
DNS Server	Sequence number of the DNS server, which is assigned automatically by the system, starting from 1.
Type	Type of DNS server, where "S" represents a statically configured DNS server, and "D" represents a DNS server obtained dynamically through DHCP.
IPv6 Address	IPv6 address of the DNS server
Interface Name	Name of the interface on the DNS server whose IP address is an IPv6 link-local address.

display ipv6 fib

Syntax **display ipv6 fib** [*ipv6-address*]

View Any view

Parameter *ipv6-address*: Destination IPv6 address whose IPv6 forwarding information base (FIB) entries are to be displayed.

Description Use the **display ipv6 fib** command to display IPv6 FIB entries. If no argument is specified, all IPv6 FIB entries will be displayed.

Example # Display all IPv6 FIB entries.

```
<Sysname> display ipv6 fib
FIB Table:
 Total number of Routes : 1

Flag:
  U:Useable   G:Gateway   H:Host   B:Blackhole   D:Dynamic   S:Static

Destination:    ::1                         PrefixLength    : 128
NextHop  :  ::1                          Flag            : HU
Label    : NULL                             Tunnel ID   : 0
TimeStamp     : Date- 12/5/2004, Time- 9:15:18
Interface    :  InLoopBack0
```

Table 172 Description on fields of the display ipv6 fib command

Field	Description
Total number of Routes	Total number of routes in the FIB
Destination	Destination address to which a packet is to be forwarded
PrefixLength	Prefix length of the destination address
NextHop	Next hop of the route to the destination

Table 172 Description on fields of the display ipv6 fib command

Field	Description
Flag	Route flag: ■ U - Usable route ■ G - Gateway route ■ H - Host route ■ B - Blackhole route ■ D - Dynamic route ■ S - Static route
Label	Label
Tunnel ID	ID of a tunnel
TimeStamp	Generation time of a FIB entry
Interface	Outgoing interface that forwards packets

display ipv6 fibcache

Syntax **display ipv6 fibcache**

View Any view

Parameter None

Description Use the **display ipv6 fibcache** command to display the total number of routes in the IPv6 FIB cache.

Example # Display the total number of routes in the IPv6 FIB cache.

```
<Sysname> display ipv6 fibcache
FIB Cache:
 Total number of Routes : 0
```

display ipv6 host

Syntax **display ipv6 host**

View Any view

Parameter None

Description Use the **display ipv6 host** command to display the mappings between host names and IPv6 addresses in the static DNS database.

Example # Display the mappings between host names and IPv6 addresses in the static DNS database.

```
<Sysname> display ipv6 host
Host                 Age          Flags          IPv6Address
aaa                  0            static          2002::1
bbb                  0            static          2002::2
```

Table 173 Description on fields of the display ipv6 host command

Field	Description
Host	Host name
Age	Time for the entry to live. "0" is displayed in the case of static configuration.
Flags	Flag indicating the type of mapping between a host name and an IPv6 address. Static indicates a static mapping.
IPv6Address	IPv6 address of a host

display ipv6 interface

Syntax **display ipv6 interface** [**brief**] [*interface-type* [*interface-number*]]

View Any view

Parameter **brief**: Displays brief IPv6 information of an interface.

interface-type: Interface type.

interface-number: Interface number.

Description Use the **display ipv6 interface** command to display the IPv6 information of an interface.

If *interface-type interface-number* is not specified, the IPv6 information of all interfaces for which IPv6 addresses can be configured is displayed; if only *interface-type* is specified, the IPv6 information of the interfaces of the specified type for which IPv6 addresses can be configured is displayed; if the *interface-type interface-number* is specified, the IPv6 information of the specified interface is displayed.

Note that:

If you have configured the time slots of a CE1/PRI or CT1/PRI interface as an ISDN PRI group using the **pri-set** command, then executing the **display ip interface brief** command only displays the time slot used by the control channel (D channel), instead of the ones used by the user channels (B channels). For details about CE1/PRI and CT1/PRI interfaces, refer to "Fundamental CE1/PRI Interface Configuration Commands" on page 201 and "Fundamental CT1/PRI Interface Configuration Commands" on page 213.

Example # Display the IPv6 information of Ethernet 1/0 for which an IPv6 address can be configured.

```
<Sysname> display ipv6 interface ethernet 1/0
Ethernet1/0 current state :UP ,
Line protocol current state :UP
```

```
IPv6 is enabled, link-local address is FE80::200:1FF:FE04:5D00
  Global unicast address(es):
    2001::1, subnet is 2001::/64
10::200:1FF:FE04:5D00, subnet is 10::/64 [AUTOCFG]
      [valid lifetime 4641s/preferred lifetime 4637s]
  Joined group address(es):
    FF02::1:FF00:1
    FF02::1:FF04:5D00
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND DAD is enabled, number of DAD attempts: 1
  ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 174 Description on fields of the display ipv6 interface command (on a router)

Field	Description
Ethernet1/0 current state	Physical state of the interface
Line protocol current state	Link layer state of the interface
IPv6 is enabled	IPv6 packet forwarding state of the interface (IPv6 packet forwarding is enabled in the example)
link-local address	Link-local address configured for the interface
Global unicast address(es)	Aggregatable global unicast address(es) configured for the interface(s)
valid lifetime	Valid lifetime of the global unicast address statelessly auto-configured
preferred lifetime	Preferred lifetime of the global unicast address statelessly auto-configured
Joined group address(es)	Address(es) of multicast group(s) that the interface joins
MTU	Maximum transmission unit of the interface
ND DAD is enabled, number of DAD attempts	Number of DAD attempts, with DAD enabled
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor solicitation (NS) message
Hosts use stateless autoconfig for addresses	Hosts use stateless autoconfiguration mode to acquire IPv6 addresses

Display brief IPv6 information of all interfaces for which IPv6 addresses can be configured.

```
<Sysname> display ipv6 interface brief
*down: administratively down
(s): spoofing
Interface                  Physical        Protocol        IPv6 Address
Ethernet1/0                up              up              2001::1
Ethernet1/1                up              down            Unassigned
```

Table 175 Description on fields of display ipv6 interface brief (on a router)

Field	Description
*down	The interface is down, that is, the interface is closed by using the **shutdown** command.

Table 175 Description on fields of display ipv6 interface brief (on a router)

Field	Description
(s)	Spoofing attribute of the interface, that is, the link protocol state of the interface is up, but the link does not exist, or the link is established on demand, instead of being permanent.
Interface	Name of the interface
Physical	Physical state of the interface
Protocol	Link protocol state of the interface
IPv6 Address	IPv6 address of the interface. Only the first of configured IPv6 addresses is displayed. (If no address is configured for the interface, "Unassigned" will be displayed.)

display ipv6 neighbors

Syntax **display ipv6 neighbors** { *ipv6-address* | **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id* } [| { **begin** | **exclude** | **include** } *string*]

View Any view

Parameter *ipv6-address*: IPv6 address whose neighbor information is to be displayed.

all: Displays information of all neighbors, including neighbors acquired dynamically and configured statically.

dynamic: Displays information of all neighbors acquired dynamically.

static: Displays information of all neighbors configured statically.

interface *interface-type interface-number*: Displays information of the neighbors of a specified interface.

vlan *vlan-id*: Displays information of the neighbors of a specified VLAN whose ID ranges from 1 to 4094.

|: Filters the output information.

begin: Displays the neighbor entries from the first one containing the specified character string.

include: Displays the neighbor entries containing the specified character string.

exclude: Displays the neighbor entries without the specified character string.

string: A case-sensitive string, consisting of 1 to 256 characters.

Description Use the **display ipv6 neighbors** command to display neighbor information.

Example # Display all neighbor information.

```
<Sysname> display ipv6 neighbors all
                Type: S-Static    D-Dynamic
```

```
IPv6 Address                Link-layer       VID  Interface     State  T   Age
FE80::200:5EFF:FE32:B800  0000-5e32-b800   N/A  Eth1/0       REACH  S   -
```

Table 176 Description on fields of the display ipv6 neighbors command

Field	Description
IPv6 Address	IPv6 address of a neighbor
Link-layer	Link layer address (MAC address of a neighbor)
VID	VLAN to which the interface connected with a neighbor belongs
Interface	Interface connected with a neighbor
State	State of a neighbor, including: ■ INCMP: The address is being resolved. The link layer address of the neighbor is unknown. ■ REACH: The neighbor is reachable. ■ STALE: The reachability of the neighbor is unknown. The device will not verify the reachability any longer unless data is sent to the neighbor. ■ DELAY: The reachability of the neighbor is unknown. The device sends an NS message after a delay. ■ PROBE: The reachability of the neighbor is unknown. The device sends an NS message to verify the reachability of the neighbor.
T	Type of neighbor information, including static configuration and dynamic acquisition.
Age	For a static entry, a hyphen "-" is displayed. For a dynamic entry, the reachable time (in seconds) elapsed is displayed, and if it is never reachable, "#" is displayed (for a neighbor acquired dynamically).

display ipv6 neighbors count

Syntax **display ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** | **vlan** *vlan-id* } **count**

View Any view

Parameter **all**: Displays the total number of all neighbor entries, including neighbor entries acquired dynamically and configured statically.

dynamic: Displays the total number of all neighbor entries acquired dynamically.

static: Displays the total number of neighbor entries configured statically.

interface *interface-type interface-number*: Displays the total number of neighbor entries of a specified interface.

vlan *vlan-id*: Displays the total number of neighbor entries of a specified VLAN whose ID ranges from 1 to 4094.

Description Use the **display ipv6 neighbors count** command to display the total number of neighbor entries satisfying the specified condition.

Example # Display the total number of neighbor entries acquired dynamically.

```
<Sysname> display ipv6 neighbors dynamic count
Total dynamic entry(ies):  2
```

display ipv6 pathmtu

Syntax **display ipv6 pathmtu** { *ipv6-address* | **all** | **dynamic** | **static** }

View Any view

Parameter *ipv6-address*: IPv6 address whose PMTU information is to be displayed.

all: Displays all PMTU information.

dynamic: Displays all dynamic PMTU information.

dynamic: Displays all static PMTU information.

Description Use the **display ipv6 pathmtu** command to display the PMTU information of IPv6 addresses.

Example # Display all PMTU information.

```
<Sysname> display ipv6 pathmtu all
IPv6 Destination Address    ZoneID  PathMTU     Age     Type
 fe80::12                   0       1300            40      Dynamic
 2222::3                    0       1280            -       Static
```

Table 177 Description on fields of the display ipv6 pathmtu command

Field	Description
IPv6 Destination Address	Destination IPv6 address
ZoneID	ID of address zone, currently invalid
PathMTU	PMTU of an IPv6 address
Age	Time for a PMTU to live. For a static PMTU, a hyphen "-" is displayed.
Type	Indicates the PMTU is dynamically negotiated or statically configured.

display ipv6 socket

Syntax **display ipv6 socket** [**socktype** *socket-type*] [*task-id socket-id*]

View Any view

Parameter **socktype** *socket-type*: Displays the socket information of this type. The socket type is in the range of 1 to 3. The value "1" represents a TCP socket, "2" a UDP socket, and "3" a raw IP socket.

task-id: Displays the socket information of the task. The task ID is in the range 1 to 100.

socket-id: Displays the information of the socket. The socket ID is in the range 0 to 3072.

Description Use the **display ipv6 socket** command to display socket information.

Example # Display the information of all sockets.

```
<Sysname> display ipv6 socket
SOCK_STREAM:
Task = VTYD(14), socketid = 4, Proto = 6,
LA = ::->22, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

Task = VTYD(14), socketid = 3, Proto = 6,
LA = ::->23, FA = ::->0,
sndbuf = 8192, rcvbuf = 8192, sb_cc = 0, rb_cc = 0,
socket option = SO_ACCEPTCONN SO_REUSEPORT SO_SENDVPNID,
socket state = SS_PRIV SS_ASYNC

SOCK_DGRAM:
SOCK_RAW:
```

Table 178 Description on fields of the display ipv6 socket command

Field	Description
SOCK_STREAM	TCP socket
SOCK_DGRAM	UDP socket
SOCK_RAW	Raw IP socket
Task	Task ID of the created socket
socketid	ID assigned by the kernel to the created socket
Proto	Protocol ID
LA	Local address and local port number
FA	Remote address and remote port number
sndbuf	Size of the send buffer
rcvbuf	Size of the receive buffer
sb_cc	Number of bytes sent by the send buffer
rb_cc	Number of bytes received by the receive buffer
socket option	Socket option set by the application
socket state	State of the socket

display ipv6 statistics

Syntax **display ipv6 statistics**

View Any view

Parameter None

Description Use the **display ipv6 statistics** command to display statistics of IPv6 packets and ICMPv6 packets.

Example # Display the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> display ipv6 statistics
  IPv6 Protocol:

    Sent packets:
      Total:      0
        Local sent out:     0            forwarded:         0
        raw packets:        0                discarded:         0
        routing failed:     0            fragments:         0
        fragments failed:   0

    Received packets:
      Total:      0
        local host:         0            hopcount exceeded: 0
        format error:       0                option error:          0
        protocol error:     0            fragments:         0
        reassembled:        0                reassembly failed: 0
        reassembly timeout: 0

  ICMPv6 protocol:

    Sent packets:
      Total:      0
        unreached:          0               too big:               0
        hopcount exceeded:  0               reassembly timeout: 0
        parameter problem:  0
        echo request:       0               echo replied:       0
        neighbor solicit:   0               neighbor advert:       0
        router solicit:     0           router advert:      0
        redirected:         0
      Send failed:
        ratelimited:        0               other errors:       0

    Received packets:
      Total:      0
        checksum error:     0          too short:          0
        bad code:           0
        unreached:          0              too big:            0
        hopcount exceeded:  0              reassembly timeout: 0
        parameter problem:  0              unknown error type: 0
        echoed:          0             echo replied:       0
        neighbor solicit:   0              neighbor advert:    0
        router solicit:     0          router advert:      0
        redirected:         0          router renumbering: 0
        unknown info type:  0
      Deliver failed:
        bad length:         0          ratelimited:        0
```

Table 179 Description on fields of the display ipv6 statistics command

Field	Description
IPv6 Protocol:	Statistics of IPv6 packets

Table 179 Description on fields of the display ipv6 statistics command

Field	Description
Sent packets: Total: 0 Local sent out: 0 forwarded: 0 raw packets: 0 discarded: 0 routing failed: 0 fragments: 0 fragments failed: 0	Statistics of sent IPv6 packets, including: ■ Total number of sent packets ■ Number of packets sent locally ■ Number of forwarded packets ■ Number of packets sent via raw socket ■ Number of discarded packets ■ Number of packets failing to be routed ■ Number of sent fragment packets ■ Number of fragments failing to be sent
Received packets: Total: 0 local host: 0 hopcount exceeded: 0 format error: 0 option error: 0 protocol error: 0 fragments: 0 reassembled: 0 reassembly failed: 0 reassembly timeout: 0	Statistics of received IPv6 packets, including ■ Total number of received packets ■ Number of packets received locally ■ Number of packets exceeding the hop limit ■ Number of packets in an incorrect format ■ Number of packets with incorrect options ■ Number of packets with incorrect protocol ■ Number of received fragment packets ■ Number of reassembled packets ■ Number of packets failing to be reassembled ■ Number of packets whose reassembly times out
ICMPv6 protocol: Sent packets: Total: 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 echo request: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 Send failed: ratelimited: 0 other errors: 0	Statistics of ICMPv6 packets Statistics of sent ICMPv6 packets, including ■ Total number of sent packets ■ Number of packets whose destination is unreachable ■ Number of too large packets ■ Number of packets exceeding the hop limit ■ Number of packets whose fragmentation and reassembly times out ■ Number of packets with parameter errors ■ Number of request packets ■ Number of response packets ■ Number of neighbor solicitation packets ■ Number of neighbor advertisement packets ■ Number of router solicit packets ■ Number of router advertisement packets ■ Number of redirected packets ■ Number of packets failing to be sent because of rate limitation ■ Number of packets with other errors

Table 179 Description on fields of the display ipv6 statistics command

Field	Description
Received packets: Total: 0 checksum error: 0 too short: 0 bad code 0 unreached: 0 too big: 0 hopcount exceeded: 0 reassembly timeout: 0 parameter problem: 0 unknown error type: 0 echoed: 0 echo replied: 0 neighbor solicit: 0 neighbor advert: 0 router solicit: 0 router advert 0 redirected: 0 router renumbering 0 unknown info type: 0 Deliver failed: bad length: 0 ratelimited: 0	Statistics of received ICMPv6 packets, including ■ Total number of received packets ■ Number of packets with checksum errors ■ Number of too small packets ■ Number of packets with error codes ■ Number of packets whose destination is unreachable ■ Number of too large packets ■ Number of packets exceeding the hop limit ■ Number of packets whose fragmentation and reassembly times out ■ Number of packets with parameter errors ■ Number of packets with unknown errors ■ Number of request packets ■ Number of response packets ■ Number of neighbor solicitation messages ■ Number of neighbor advertisement packets ■ Number of router solicitation packets ■ Number of router advertisement packets ■ Number of redirected packets ■ Number of packets recounted by the router ■ Number of unknown type of packets ■ Number of packets with a incorrect size ■ Number of packets failing to be received because of rate limitation

display tcp ipv6 statistics

Syntax **display tcp ipv6 statistics**

View Any view

Parameter None

Description Use the **display tcp ipv6 statistics** command to display TCP connection statistics.

Example # Display the statistics of IPv6 TCP connections.

```
<Sysname> display tcp ipv6 statistics
Received packets:
     Total: 0
     packets in sequence: 0 (0 bytes)
     window probe packets: 0, window update packets: 0
     checksum error: 0, offset error: 0, short error: 0

     duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes)
```

```
     out-of-order packets: 0 (0 bytes)
     packets with data after window: 0 (0 bytes)
     packets after close: 0

     ACK packets: 0 (0 bytes)
     duplicate ACK packets: 0, too much ACK packets: 0

Sent packets:
     Total: 0
     urgent packets: 0
     control packets: 0 (including 0 RST)
     window probe packets: 0, window update packets: 0

     data packets: 0 (0 bytes) data packets retransmitted: 0 (0 bytes)
     ACK only packets: 0 (0 delayed)

Retransmitted timeout: 0, connections dropped in retransmitted timeout: 0
Keepalive timeout: 0, keepalive probe: 0, keepalive timeout, so connections di
sconnected : 0
Initiated connections: 0, accepted connections: 0, established connections: 0
Closed connections: 0 (dropped: 0, initiated dropped: 0)
```

Table 180 Description on fields of the display tcp ipv6 statistics command

Field	Description
Received packets: Total: 0 packets in sequence: 0 (0 bytes) window probe packets: 0 window update packets: 0 checksum error: 0 offset error: 0 short error: 0 duplicate packets: 0 (0 bytes), partially duplicate packets: 0 (0 bytes) out-of-order packets: 0 (0 bytes) packets with data after window: 0 (0 bytes) packets after close: 0 ACK packets: 0 (0 bytes) duplicate ACK packets: 0 too much ACK packets: 0	Statistics of received packets, including ■ Total number of received packets ■ Number of packets received in sequence ■ Number of window probe packets ■ Number of window size update packets ■ Number of packets with checksum errors ■ Number of packets with offset errors ■ Number of packets whose total length is less than specified by the packet header ■ Number of duplicate packets ■ Number of partially duplicate packets ■ Number of out-of-order packets ■ Number of packets exceeding the size of the receiving window ■ Number of packets received after the connection is closed ■ Number of ACK packets ■ Number of duplicate ACK packets ■ Number of excessive ACK packets

Table 180 Description on fields of the display tcp ipv6 statistics command

Field	Description
Sent packets:	Statistics of sent packets, including
Total: 0	**1** Total number of packets
urgent packets: 0	**2** Number of packets containing an urgent indicator
control packets: 0 (including 0 RST)	**3** Number of control packets
window probe packets: 0	**4** Number of window probe packets
window update packets: 0	**5** Number of window update packets
data packets: 0 (0 bytes) data	**6** Number of data packets
packets retransmitted: 0 (0 bytes)	**7** Number of retransmitted packets
ACK only packets: 0 (0 delayed)	**8** Number of ACK packets
Retransmitted timeout	Number of packets whose retransmission times out
connections dropped in retransmitted timeout	Number of connections dropped because of retransmission timeout
Keepalive timeout	Number of keepalive timeouts
keepalive probe	Number of keepalive probes
Keepalive timeout, so connections disconnected	Number of connections dropped because of keepalive response timeout
Initiated connections	Number of initiated connections
accepted connections	Number of accepted connections
established connections	Number of established connections
Closed connections	Number of closed connections
dropped	Number of dropped connections (after SYN is received from the peer)
initiated dropped	Number of initiated but dropped connections (before SYN is received from the peer)

display tcp ipv6 status

Syntax **display tcp ipv6 status**

View Any view

Parameter None

Description Use the **display tcp ipv6** command to display the TCP connection status.

Example # Display the TCP connection status.

```
<Sysname> display tcp ipv6 status
TCP6CB       Local Address       Foreign Address      State
045d8074     ::->21                ::->0              Listening
```

Table 181 Description on fields of the display tcp ipv6 status command

Field	Description
TCP6CB	IPv6 address of the TCP control block (hexadecimal)
Local Address	Local IPv6 address
Foreign Address	Remote IPv6 address
State	IPv6 TCP connection status, including ■ Closed ■ Listening ■ Syn_Sent ■ Syn_Rcvd ■ Established ■ Close_Wait ■ Fin_Wait1 ■ Closing ■ Last_Ack ■ Fin_Wait2 ■ Time_Wait

display udp ipv6 statistics

Syntax **display udp ipv6 statistics**

View Any view

Parameter None

Description Use the **display udp ipv6 statistics** command to display statistics of UDP packets.

Example # Display statistics information of UDP packets.

```
<Sysname> display udp ipv6 statistics
Received packets:
     Total: 0
     checksum error: 0
     shorter than header: 0, data length larger than packet: 0
     unicast(no socket on port): 0
     broadcast/multicast(no socket on port): 0
     not delivered, input socket full: 0
     input packets missing pcb cache: 0
Sent packets:
     Total: 0
```

Table 182 Description on fields of the display udp ipv6 statistics command

Field	Description
Total	Total number of received/sent packets
checksum error	Total number of packets with a checksum error

Table 182 Description on fields of the display udp ipv6 statistics command

Field	Description
shorter than header	Total number of UDP packets whose total length is less than specified by the packet header
data length larger than packet	Total number of packets whose data length exceeds that specified by the packet header
unicast(no socket on port)	Total number of unicast packets without any socket received on a port
broadcast/multicast(no socket on port)	Total number of broadcast/multicast packets without any socket received on a port
not delivered, input socket full	Number of packets not handled because of the receive buffer being full
input packet missing pcb cache	Number of packets failing to match the PCB cache

dns server ipv6

Syntax **dns server ipv6** *ipv6-address* [*interface-type interface-number*]

undo dns server ipv6 *ipv6-address* [*interface-type interface-number*]

View System view

Parameter *ipv6-address*: IPv6 address of a DNS server.

interface-type interface-number: Specifies an interface. When the IPv6 address of the DNS server is a link-local address, this argument must be specified.

Description Use the **dns server ipv6** command to configure an IPv6 address for a DNS server.

Use the **undo dns server ipv6** command to remove the configured DNS server.

By default, no DNS server is configured.

Example # Configure the IPv6 address 2002::1 for a DNS server.

```
<Sysname> system-view
[Sysname] dns server ipv6 2002::1
```

ipv6

Syntax **ipv6**

undo ipv6

View System view

Parameter None

Description Use the **ipv6** command to enable the IPv6 packet forwarding function.

Use the **undo ipv6** command to disable the IPv6 packet forwarding function.

By default, the IPv6 packet forwarding function is disabled.

Example # Enable the IPv6 packet forwarding function.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address

Syntax **ipv6 address** { *ipv6-address prefix-length* | *ipv6-prefix*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-prefix*/*prefix-length*]

View Interface view

Parameter *ipv6-address*: IPv6 address.

ipv6-prefix: Prefix of an IPv6 address.

prefix-length: Prefix length of an IPv6 address, in the range 1 to 128.

Description Use the **ipv6 address** command to configure an IPv6 site-local address or aggregatable global unicast address for an interface.

Use the **undo ipv6 address** command to remove the IPv6 address from the interface.

By default, no site-local address or global unicast address is configured for an interface.

Note that except the link-local address automatically configured and the one generated through stateless autoconfiguration, all IPv6 addresses will be removed from the interface if you carry out the **undo ipv6 address** command without any parameter specified.

Example # Set the aggregatable global IPv6 unicast address of Ethernet1/0 to 2001::1/64.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] ipv6 address 2001::1/64
```

ipv6 address auto link-local

Syntax **ipv6 address auto link-local**

undo ipv6 address auto link-local

View Interface view

Parameter None

Description Use the **ipv6 address auto link-local** command to automatically generate a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically generated link-local address for an interface.

By default, a link-local address will automatically be generated after a site-local or global IPv6 unicast address is configured for an interface.

Example # Configure Ethernet1/0 to automatically generate a link-local address.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 address auto link-local
```

ipv6 address eui-64

Syntax **ipv6 address** *ipv6-prefix*/*prefix-length* **eui-64**

undo ipv6 address *ipv6-prefix*/*prefix-length* **eui-64**

View Interface view

Parameter *ipv6-prefix*/*prefix-length*: IPv6 address prefix and prefix length. They together specify the prefix of an IPv6 address in the EUI-64 format.

Description Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format for an interface.

Use the **undo ipv6 address eui-64** command to remove the configured site-local address or global unicast address in the EUI-64 format for the interface.

By default, no site-local or global unicast address in EUI-64 format is configured for an interface.

Example # Configure an IPv6 address in the EUI-64 format for Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

Syntax **ipv6 address** *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View Interface view

Parameter *ipv6-address*: IPv6 link-local address. The first ten bits of an address must be 1111111010 (binary), that is, the first group of hexadecimals in the address must be FE80 to FEBF.

Description Use the **ipv6 address link-local** command to configure a link-local address manually for a specified interface.

Use the **undo ipv6 address link-local** command to remove the configured link-local address for the interface.

Example # Configure a link-local address for Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 address fe80::1 link-local
```

ipv6 fibcache

Syntax **ipv6 fibcache**

undo ipv6 fibcache

View System view

Parameter None

Description Use the **ipv6 fibcache** command to enable the caching function of the IPv6 FIB.

Use the **undo ipv6 fibcache** command to disable the caching function of the IPv6 FIB.

By default, the caching function of the IPv6 FIB is disabled.

Note that the caching function of the IPv6 FIB is valid only for packets to be forwarded.

Example # Enable the caching function of the IPv6 FIB.

```
<Sysname> system-view
[Sysname] ipv6 fibcache
```

ipv6 fib-loadbalance-type hash-based

Syntax **ipv6 fib-loadbalance-type hash-based**

undo ipv6 fib-loadbalance-type hash-based

View System view

Parameter None

Description Use the **ipv6 fib-loadbalance-type hash-based** command to specify the load sharing mode based on the HASH algorithm for packet forwarding.

Use the **undo ipv6 fib-loadbalance-type hash-based** command to restore the load sharing mode to the default.

By default, the load sharing based on polling is adopted, that is, each ECMP route is used in turn to forward packets.

Example # Specify the load sharing mode based on the HASH algorithm for packet forwarding.

```
<Sysname> system-view
[Sysname] ipv6 fib-loadbalance-type hash-based
```

ipv6 host

Syntax **ipv6 host** *hostname ipv6-address*

undo ipv6 host *hostname* [*ipv6-address*]

View System view

Parameter *hostname*: Host name, a string of up to 20 characters. The character string can contain letters, numerals, "_", "-", or "." and must contain at least one letter.

ipv6-address: IPv6 address.

Description Use the **ipv6 host** command to configure the mappings between host names and IPv6 addresses.

Use the **undo ipv6 host** command to remove the mappings between host names and IPv6 addresses.

Each host name can correspond to only one IPv6 address.

Example # Configure the mapping between a host name and an IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 host aaa 2001::1
```

ipv6 icmp-error

Syntax **ipv6 icmp-error** { **bucket** *bucket-size* | **ratelimit** *interval* } *

undo ipv6 icmp-error

View System view

Parameter **bucket** *bucket-size*: Number of tokens in a token bucket, in the range of 1 to 200.

ratelimit *interval*: Update period of the token bucket in milliseconds, in the range of 0 to 2,147,483,647. The update period "0" indicates that the number of ICMPv6 error packets sent is not restricted.

Description Use the **ipv6 icmp-error** command to configure the size and update period of a token bucket.

Use the **undo ipv6 icmp-error** command to restore the defaults.

By default, the size is 10 and the update period is 100 milliseconds. That is, at most 10 ICMPv6 error packets can be sent within these 100 milliseconds.

Example # Set the capacity of the token bucket to 50 and the update period to 100 milliseconds.

```
<Sysname> system-view
[Sysname] ipv6 icmp-error bucket 50 ratelimit 100
```

ipv6 icmpv6 multicast-echo-reply enable

Syntax ipv6 icmpv6 multicast-echo-reply enable

undo ipv6 icmpv6 multicast-echo-reply

View System view

Parameters None

Description Use the **ipv6 icmpv6 multicast-echo-reply enable** command to enable sending of multicast echo replies.

Use the **undo ipv6 icmpv6 multicast-echo-reply** command to disable sending of multicast echo replies.

By default, the device is disabled from sending multicast echo replies.

Examples # Enable sending of multicast echo replies.

```
<Sysname> system-view
[Sysname] ipv6 icmpv6 multicast-echo-reply enable
```

ipv6 mtu

Syntax **ipv6 mtu** *mtu-size*

undo ipv6 mtu

View Interface view

Parameter *mtu-size*: Size of the maximum transmission units (MTUs) of an interface in bytes, in the range of 1,280 to 1,500. The default value is 1,500.

Description Use the **ipv6 mtu** command to set the MTU of IPv6 packets sent over an interface.

Use the **undo ipv6 mtu** command to restore the default MTU.

Set the MTU of IPv6 packets sent over Ethernet1/0 to 1280 bytes.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 mtu 1280
```

ipv6 nd autoconfig managed-address-flag

Syntax **ipv6 nd autoconfig managed-address-flag**

undo ipv6 nd autoconfig managed-address-flag

View Interface view

Parameter None

Description Use the **ipv6 nd autoconfig managed-address-flag** command to set the managed address configuration (M) flag to 1 so that the host can acquire an IPv6 address through stateful autoconfiguration (for example, DHCP server).

Use the **undo ipv6 nd autoconfig managed-address-flag** command to restore the M flag to the default value "0" so that the host can acquire an IPv6 address through stateless autoconfiguration.

By default, the M flag is set to 0.

Example # Configure the host to acquire an IPv6 address through stateful autoconfiguration.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd autoconfig managed-address-flag
```

ipv6 nd autoconfig other-flag

Syntax **ipv6 nd autoconfig other-flag**

undo ipv6 nd autoconfig other-flag

View Interface view

Parameter None

Description Use the **ipv6 nd autoconfig other-flag** command to set the other stateful configuration flag (O) flag to 1 so that the host can acquire information other than IPv6 address through stateful autoconfiguration (for example, DHCP server).

Use the **undo ipv6 nd autoconfig other-flag** command to remove the setting so that the host can acquire other information through stateless autoconfiguration.

By default, the O flag is set to 0.

Example # Configure the host to acquire information other than IPv6 address through stateless autoconfiguration.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo ipv6 nd autoconfig other-flag
```

ipv6 nd dad attempts

Syntax **ipv6 nd dad attempts** *value*

undo ipv6 nd dad attempts

View Interface view

Parameter *value*: Number of attempts to send an NS message for DAD, in the range of 0 to 600. The default value is "1". When it is set to 0, the DAD is disabled.

Description Use the **ipv6 nd dad attempts** command to configure the number of attempts to send an NS message for DAD.

Use the **undo ipv6 nd dad attempts** command to restore the default.

By default, the number of attempts to send an NS message for DAD is 1.

Example # Set the number of attempts to send an NS message for DAD to 20.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd dad attempts 20
```

ipv6 nd hop-limit

Syntax **ipv6 nd hop-limit** *value*

undo ipv6 nd hop-limit

View System view

Parameter *value*: Number of hops, in the range of 0 to 255. When it is set to 0, the Cur Hop Limit field in RA messages sent by the device is 0. That is, the number of hops is determined by the host itself, but not specified by the device.

Description Use the **ipv6 nd hop-limit** command to configure the hop limit advertised by the device.

Use the **undo ipv6 nd hop-limit** command to restore the default hop limit.

By default, the hop limit advertised by the device is 64.

Example # Set the hop limit advertised by the device to 100.

```
<Sysname> system-view
[Sysname] ipv6 nd hop-limit 100
```

ipv6 nd ns retrans-timer

Syntax **ipv6 nd ns retrans-timer** *value*

undo ipv6 nd ns retrans-timer

View Interface view

Parameter *value*: Interval for sending NS messages in milliseconds, in the range of 1,000 to 3,600,000.

Description Use the **ipv6 nd ns retrans-timer** command to set the interval for sending NS messages. The local interface sends NS messages at intervals of this value. Furthermore, the Retrans Timer field in RA messages sent by the local interface is equal to this value.

Use the **undo ipv6 nd ns retrans-timer** command to restore the default interval.

By default, the local interface sends NS messages at intervals of 1,000 milliseconds and the Retrans Timer field in RA messages sent by the local interface is 0.

Example # Specify Ethernet1/0 to send NS messages at intervals of 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd ns retrans-timer 10000
```

ipv6 nd nud reachable-time

Syntax **ipv6 nd nud reachable-time** *value*

undo ipv6 nd nud reachable-time

View Interface view

Parameter *value*: Neighbor reachable time in milliseconds, in the range of 1 to 3,600,000.

Description Use the **ipv6 nd nud reachable-time** command to configure the neighbor reachable time on an interface. This time value serves as not only the neighbor reachable time on the local interface, but also the value of the Reachable Timer field in RA messages sent by the local interface.

Use the **undo ipv6 nd nud reachable-time** command to restore the default neighbor reachable time and to specify the value of the Reachable Timer field in RA messages as 0, so that the number of hops is determined by the host itself, but not specified by the device.

By default, the neighbor reachable time on the local interface is 30,000 milliseconds and the Reachable Timer field in RA messages is 0.

Example # Set the neighbor reachable time on Ethernet1/0 to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd nud reachable-time 10000
```

ipv6 nd ra halt

Syntax **ipv6 nd ra halt**

undo ipv6 nd ra halt

View Interface view

Parameter None

Description Use the **ipv6 nd ra halt** command to enable RA message suppression.

Use the **undo ipv6 nd ra halt** command to disable the RA message suppression.

By default, RA messages are suppressed.

Example

- On a switch

Suppress RA messages on Vlan-interface100.

```
<Sysname> system-view
[Sysname] interface vlan-interface 100
[Sysname-Vlan-interface100] ipv6 nd ra halt
```

- On a router

Suppress RA messages on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd ra halt
```

ipv6 nd ra interval

Syntax **ipv6 nd ra interval** *max-interval-value min-interval-value*

undo ipv6 nd ra interval

View Interface view

Parameter *max-interval-value*: Maximum interval for advertising RA messages in seconds, in the range of 4 to 1,800.

min-interval-value: Minimum interval for advertising RA messages in seconds, in the range of 3 to 1,350.

Description Use the **ipv6 nd ra interval** command to set the maximum and minimum interval for advertising RA messages. The device advertises RA messages at intervals of a random value between the maximum interval and the minimum interval.

Use the **undo ipv6 nd ra interval** command to restore the default.

By default, the maximum interval between RA messages is 600 seconds, and the minimum interval is 200 seconds.

Note the following:

- The minimum interval should be three-fourths of the maximum interval or less.
- The maximum interval for sending RA messages should be less than or equal to the router lifetime in RA messages.

Example # Set the maximum interval for advertising RA messages to 1,000 seconds and the minimum interval to 700 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd ra interval 1000 700
```

ipv6 nd ra prefix

Syntax **ipv6 nd ra prefix** { *ipv6-prefix prefix-length* | *ipv6-prefix*/*prefix-length* } *valid-lifetime preferred-lifetime* [**no-autoconfig** | **off-link**] *

undo ipv6 nd ra prefix *ipv6-prefix*

View Interface view

Parameter *prefix-length*: Prefix length of an IPv6 address.

ipv6-prefix: IPv6 address prefix.

valid-lifetime: Valid lifetime of a prefix in seconds, in the range of 0 to 4,294,967,295.

preferred-lifetime: Preferred lifetime of a prefix used for stateless autoconfiguration in seconds, in the range of 0 to 4,294,967,295.

no-autoconfig: Specifies a prefix not to be used for stateless autoconfiguration. If this keyword is not provided, the prefix is used for stateless autoconfiguration.

off-link: Specifies the address with the prefix not to be directly reachable on the link. If this keyword is not provided, the address with the prefix is directly reachable on the link.

Description Use the **ipv6 nd ra prefix** command to configure the prefix information in RA messages.

Use the **undo ipv6 nd ra prefix** command to remove the prefix information from RA messages.

By default, no prefix information is configured in RA messages and the IPv6 address of the interface sending RA messages is used as the prefix information.

Example # Configure the prefix information for RA messages on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd ra prefix 2001:10::100/64 100 10
```

ipv6 nd ra router-lifetime

Syntax **ipv6 nd ra router-lifetime** *value*

undo ipv6 nd ra router-lifetime

View Interface view

Parameter *time*: Router lifetime in seconds, in the range of 0 to 9,000. When it is set to 0, the device does not serve as the default router.

Description Use the **ipv6 nd ra router-lifetime** command to configure the router lifetime in RA messages.

Use the **undo ipv6 nd ra router-lifetime** command to restore the default configuration.

By default, the router lifetime in RA messages is 1,800 seconds.

Note that the router lifetime in RA messages should be greater than or equal to the advertising interval.

Example # Set the router lifetime in RA messages on Ethernet1/0 to 1,000 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 nd ra router-lifetime 1000
```

ipv6 neighbor

Syntax **ipv6 neighbor** *ipv6-address mac-address* { *vlan-id port-type port-number* | **interface** *interface-type interface-number* }

undo ipv6 neighbor *ipv6-address interface-type interface-number*

View System view

Parameter *ipv6-address*: IPv6 address in a static neighbor entry.

mac-address: Link layer address in a static neighbor entry (48 bits long, in the format of H-H-H).

vlan-id: VLAN ID in a static neighbor entry, in the range of 1 to 4094.

port-type port-number: Type and number of a Layer 2 port in a static neighbor entry.

interface *interface-type interface-number*: Type and number of a Layer 3 interface in a static neighbor entry.

Description Use the **ipv6 neighbor** command to configure a static neighbor entry.

Use the **undo ipv6 neighbor** command to remove a static neighbor entry.

Note that you can adopt the IPv6 address and link layer address of the Layer 3 VLAN interface or those of the VLAN port to configure a static neighbor entry.

- If a static neighbor entry is configured by using the first method, the neighbor entry is in the INCMP state. After the device obtains the corresponding Layer 2 VLAN port information through resolution, the neighbor entry will go into the REACH state.
- If a static neighbor entry is configured by using the second method, the corresponding VLAN interface must exist and the port specified by *port-type port-number* must belong to the VLAN specified by *vlan-id*. After a static neighbor entry is configured, the device will relate the VLAN interface with the IPv6 address to identify a static neighbor entry uniquely and the entry will be in the REACH state.

You only need to specify the corresponding VLAN interface before removing a static neighbor entry.

Example # Configure a static neighbor entry for Layer 3 interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] ipv6 neighbor 2000::1 fe-e0-89 interface ethernet1/0
```

ipv6 neighbors max-learning-num

Syntax **ipv6 neighbors max-learning-num** *number*

undo ipv6 neighbors max-learning-num

View Interface view

Parameter *number*: Maximum number of neighbors that can be dynamically learned by an interface, in the range of 1 to 2,048. The default value is 1,024.

Description Use the **ipv6 neighbors max-learning-num** command to configure the maximum number of neighbors that can be dynamically learned on a specified interface.

Use the **undo ipv6 neighbors max-learning-num** command to restore the default.

Example # Set the maximum number of neighbors that can be dynamically learned on Ethernet1/0 to 10.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 neighbors max-learning-num 10
```

ipv6 pathmtu

Syntax **ipv6 pathmtu** *ipv6-address* [*value*]

undo ipv6 pathmtu *ipv6-address*

View System view

Parameter *ipv6-address*: Specified IPv6 address.

value: PMTU of a specified IPv6 address in bytes, in the range of 1,280 to 10,000.

Description Use the **ipv6 pathmtu** command to configure a static PMTU for a specified IPv6 address.

Use the **undo ipv6 pathmtu** command to remove the PMTU configuration for a specified IPv6 address.

By default, no static PMTU is configured.

Example # Configure a static PMTU for a specified IPv6 address.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu fe80::12 1300
```

ipv6 pathmtu age

Syntax **ipv6 pathmtu age** *age-time*

undo ipv6 pathmtu age

View System view

Parameter *age-time*: Aging time for PMTU in minutes, in the range of 10 to 100.

Description Use the **ipv6 pathmtu age** command to configure the aging time for a dynamic PMTU.

Use the **undo ipv6 pathmtu age** command to restore the default.

By default, the aging time is 10 minutes.

Note that the aging time is invalid for a static PMTU.

Related command: **display ipv6 pathmtu**.

Example # Set the aging time for a dynamic PMTU to 40 minutes.

```
<Sysname> system-view
[Sysname] ipv6 pathmtu age 40
```

reset dns ipv6 dynamic-host

Syntax **reset dns ipv6 dynamic-host**

View User view

Parameter None

Description Use the **reset dns ipv6 dynamic-host** command to clear IPv6 dynamic domain name cache information.

Example # Clear IPv6 dynamic domain name cache information.

```
<Sysname> reset dns ipv6 dynamic-host
```

reset ipv6 fibcache

Syntax **reset ipv6 fibcache**

View User view

Parameter None

Description Use the **reset ipv6 fibcache** command to clear FIB cache entries.

Example # Clear FIB cache entries.

```
<Sysname> reset ipv6 fibcache
```

reset ipv6 neighbors

Syntax **reset ipv6 neighbors** { **all** | **dynamic** | **interface** *interface-type interface-number* | **static** }

View User view

Parameter **all**: Clears the static and dynamic neighbor information on all interfaces.

dynamic: Clears the dynamic neighbor information on all interfaces.

interface *interface-type interface-number*: Clears dynamic neighbor information on a specified interface.

static: Clears the static neighbor information on all interfaces.

Description Use the **reset ipv6 neighbors** command to clear IPv6 neighbor information.

Example # Clear neighbor information on all interfaces.

```
<Sysname> reset ipv6 neighbors all
```

reset ipv6 pathmtu

Syntax **reset ipv6 pathmtu** { **all** | **static** | **dynamic** }

View User view

Parameter **all**: Clears all PMTUs.

static: Clears all static PMTUs.

dynamic: Clears all dynamic PMTUs.

Description Use the **reset ipv6 pathmtu** the command to clear the PMTU information.

Example # Clear all PMTUs.

```
<Sysname> reset ipv6 pathmtu all
```

reset ipv6 statistics

Syntax **reset ipv6 statistics**

View User view

Parameter None

Description Use the **reset ipv6 statistics** command to clear the statistics of IPv6 packets and ICMPv6 packets.

Example # Clear the statistics of IPv6 packets and ICMPv6 packets.

```
<Sysname> reset ipv6 statistics
```

reset tcp ipv6 statistics

Syntax **reset tcp ipv6 statistics**

View User view

Parameter None

Description Use the **reset tcp ipv6 statistics** command to clear the statistics of all TCP connections.

Example # Clear the statistics of all TCP connections.

```
<Sysname> reset tcp ipv6 statistics
```

reset udp ipv6 statistics

Syntax **reset udp ipv6 statistics**

View User view

Parameter None

Description Use the **reset udp ipv6 statistics** command to clear the statistics of all UDP packets.

Example # Clear the statistics of all UDP packets.

```
<Sysname> reset udp ipv6 statistics
```

tcp ipv6 timer fin-timeout

Syntax **tcp ipv6 timer fin-timeout** *wait-time*

undo tcp ipv6 timer fin-timeout

View System view

Parameter *wait-time*: Length of the finwait timer for TCP connections in seconds, in the range of 76 to 3,600.

Description Use the **tcp ipv6 timer fin-timeout** command to set the finwait timer for TCP connections.

Use the **undo tcp ipv6 timer fin-timeout** command to restore the default finwait timer length.

By default, the length of the finwait timer is 675 seconds.

Example # Set the finwait timer length of TCP connections to 800 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer fin-timeout 800
```

tcp ipv6 timer syn-timeout

Syntax **tcp ipv6 timer syn-timeout** *wait-time*

undo tcp ipv6 timer syn-timeout

View System view

Parameter *wait-time*: Length of the synwait timer for TCP connections in seconds, in the range of 2 to 600.

Description Use the **tcp ipv6 timer syn-timeout** command to set the synwait timer for TCP connections

Use the **undo tcp ipv6 timer syn-timeout** command to restore the default synwait timer length.

By default, the length of the synwait timer of TCP connections is 75 seconds.

Example # Set the synwait timer length of TCP connections to 100 seconds.

```
<Sysname> system-view
[Sysname] tcp ipv6 timer syn-timeout 100
```

tcp ipv6 window

Syntax **tcp ipv6 window** *size*

undo tcp ipv6 window

View System view

Parameter *size*: Size of the TCP sending/receiving buffer in KB (kilobyte), in the range of 1 to 32.

Description Use the **tcp ipv6 window** command to set the size of the TCP sending/receiving buffer.

Use the **undo tcp ipv6 window** command to restore the default.

By default, the size of the TCP sending/receiving buffer is 8 KB.

Example # Set the size of the TCP sending/receiving buffer to 4 KB.

```
<Sysname> system-view
[Sysname] tcp ipv6 window 4
```

66 NAT-PT CONFIGURATION COMMANDS

display natpt address-group

Syntax **display natpt address-group**

View Any view

Parameter None

Description Use the **display natpt address-group** command to display the configuration information of a NAT-PT address pool.

Example # Display the configuration information of a NAT-PT address pool.

```
<Sysname> display natpt address-group
 NATPT IPv4 Address Pool Information:
 1: from 1.1.1.1        to 1.1.1.4
```

Table 183 Description on fields of the display natpt address-group command

Field	Description
1:	Address pool number
from 1.1.1.1	Start address in an address pool
to 1.1.1.4	End address in an address pool

display natpt address-mapping

Syntax **display natpt address-mapping**

View Any view

Parameter None

Description Use the **display natpt address-mapping** command to display the static and dynamic NAT-PT mappings.

The displayed information does not include the information about port translation through the NAPT-PT mechanism.

Example # Display the static and dynamic NAT-PT mapping.

```
<Sysname> display natpt address-mapping
NATPT address mapping(v6bound view):
 IPv4 Address       IPv6 Address                        Type
 1.1.1.1            3001::0001                          SOURCE
 2.2.2.2            3001::0002                          DESTINATION

 NATPT V6Server static mapping:
 IPv4Address              IPv6 Address                    Pro
 1.1.1.1^    6            3001::0003^    1270             TCP
```

Table 184 Description on fields of the display natpt address-mapping command

Field	Description
NATPT address mapping (v6bound view)	Displays the static and dynamic IPv6-to-IPv4 mapping.
Type	Indicates whether the connection is initiated by an IPv6 host or an IPv4 host. If initiated by an IPv6 host, the IPv6 address is the source address. Otherwise, it is the destination address. In the example, 3001::0001 is the source address and 2.2.2.2 is the destination address.
NATPT V6Server static mapping	Displays the NAT-PT address/port mapping.
IPv4Address	IPv4 address and port number
IPv6 Address	IPv6 address and port number
Pro	Protocol type

display natpt aging-time

Syntax **display natpt aging-time**

View Any view

Parameter None

Description Use the **display natpt aging-time** command to display the timeout time for a NAT-PT connection.

Example # Display the timeout time for a NAT-PT session.

```
<Sysname> display natpt aging-time

 NATPT aging-time value information:
      tcp -------aging-time value is     86400 (seconds)
      udp -------aging-time value is     40 (seconds)
     icmp -------aging-time value is     20 (seconds)
      dns -------aging-time value is     10 (seconds)
      syn -------aging-time value is     240 (seconds)
   finrst -------aging-time value is     5 (seconds)
     frag -------aging-time value is     5 (seconds)
```

Table 185 Description on fields of the display natpt aging-time command

Field	Description
tcp -------aging-time value is 86400	The timeout time for a TCP packet is 86400 seconds.
udp -------aging-time value is 40	The timeout time for a UDP packet is 40 seconds.

Table 185 Description on fields of the display natpt aging-time command

Field	Description
icmp -------aging-time value is 20	The timeout time for an ICMP packet is 20 seconds.
dns -------aging-time value is 10	The timeout time for a DNS packet is 10 seconds.
syn -------aging-time value is 240	The timeout time for a synchronization packet is 240 seconds.
finrst -------aging-time value is 5	The timeout time for a finrst packet is 5 seconds.
frag -------aging-time value is 5	The timeout time for a fragmented packet is 5 seconds.

display natpt all

Syntax **display natpt all**

View Any view

Parameter None

Description Use the **display natpt all** command to display all NAT-PT configuration information.

Example # Display all NAT-PT configuration information.

```
<Sysname> display natpt all
NATPT IPv4 Address Pool Information:
 1: from 1.1.1.1        to 1.1.1.4

NATPT address mapping(v6bound view):
 IPv4 Address       IPv6 Address                      Type
 1.1.1.1            3001::0001                        SOURCE
 2.2.2.2            3001::0002                        DESTINATION

 NATPT V6Server static mapping:
 IPv4Address              IPv6 Address                  Pro
 1.1.1.1^    6            3001::0003^    1270           TCP

 NATPT V4bound information:
 No Dynamic V4 Address Records Present

 NATPT V6bound information:
 No Dynamic V6 Address Records Present

 NATPT Prefix Info:
 Prefix                                Interface       NextHop
 2001::

 NATPT aging-time value information:
      tcp -------aging-time value is  86400 (seconds)
      udp -------aging-time value is     40 (seconds)
     icmp -------aging-time value is     20 (seconds)
      dns -------aging-time value is     10 (seconds)
      syn -------aging-time value is    240 (seconds)
```

```
  finrst -------aging-time value is      5 (seconds)
    frag -------aging-time value is      5 (seconds)

NATPT Statistics:
        Total Sessions:   0
        Expired Sessions: 0
        Hits:             0
        Misses:           0
        Total Fragment Sessions:   0
        Expired Fragment Sessions: 0
        Fragment Hits:             0
        Fragment Misses:           0
        Total Address Mapping:   0 (static: 0  dynamic: 0 )
        Total V6Server Mappings: 0

NATPT Interfaces:
         Ethernet1/0
```

For the explanations to the information displayed above, see the descriptions of related commands.

display natpt frag-sessions

Syntax **display natpt frag-sessions**

View Any view

Parameter None

Description Use the **display natpt frag-sessions** command to display the NAT-PT fragment session information.

Example # Display the NAT-PT fragment session information.

```
<Sysname> display natpt frag-sessions
 NATPT Fragment-Session Info:
 No                    IPV6Source              IPV4Source        PacketID
                       IPV6Destination         IPV4Destination
 No Fragment-Sessions Present
```

Table 186 Description on fields of the display natpt frag-sessions command

Field	Description
No	Serial number
IPv6 Source	Source IPv6 address
IPv6 Destination	Destination IPv6 address
IPv4 Source	Source IPv4 address
IPv4 Destination	Destination IPv4 address
PacketID	Serial number of a fragmented packet

display natpt session

Syntax **display natpt session { all | icmp | tcp | udp }**

View Any view

Parameter **all**: Displays the information of all sessions.

icmp: Displays the information of ICMP sessions.

tcp: Displays the information of TCP sessions.

udp: Displays the information of UDP sessions.

Description Use the **display natpt session** command to display the information of dynamic NAT-PT sessions.

Example # Display the information of all dynamic NAT-PT sessions.

```
<Sysname> display natpt session all
 NATPT Session Info:
 No                    IPV6Source              IPV4Source              Pro
                       IPV6Destination         IPV4Destination
 No Sessions Present
```

Table 187 Description on fields of the display natpt session command

Field	Description
No	Serial number
IPV6Source	Source IPv6 address
IPV6Destination	Destination IPv6 address
IPV4 Source	Source IPv4 address
IPV4 Destination	Destination IPv4 address
Pro	Protocol type

display natpt statistics

Syntax **display natpt statistics**

View Any view

Parameter None

Description Use the **display natpt statistics** command to display NAT-PT statistics information.

The statistics information does not include information about port translation through NAPT-PT mechanism.

Example # Display NAT-PT statistics information.

```
<Sysname> display natpt statistics
 NATPT Statistics:
         Total Sessions:    0
         Expired Sessions:  0
         Hits:              0
         Misses:            0
         Total Fragment Sessions:       0
         Expired Fragment Sessions:     0
         Fragment Hits:                 0
         Fragment Misses:               0
         Total Address Mapping:         0 (static: 0  dynamic: 0 )
         Total V6Server Mappings:       0

 NATPT Interfaces:
          Ethernet1/0
```

Table 188 Description on fields of the display natpt statistic command

Field	Description
Total Sessions	Total number of sessions
Expired Session	Number of expired sessions
Hits	Number of successful NAT-PT transactions
Misses	Number of failed NAT-PT transactions
Total Fragment Sessions	Total number of active fragment sessions
Expired Fragment Sessions	Number of expired fragment sessions
Fragment Hits	Number of successful fragment sessions
Fragment Misses	Number of failed fragment sessions
Total Address Mappings	Number of static and dynamic mappings
Total V6Server Mappings	Number of V6Server mappings (address/port mappings)
NATPT Interfaces: Ethernet1/0	NAT-PT enabled interface

natpt address-group

Syntax **natpt address-group** *group-number start-ipv4-address end-ipv4-address*

undo natpt address-group *group-number*

View System view

Parameter *group-number*: Number of an address pool, in the range of 1 to 31.

start-ipv4-address: Start IPv4 address in a pool.

end-ipv4-address: End IPv4 address in a pool.

Description Use the **natpt address-group** command to configure a NAT-PT address pool.

Use the **undo natpt address-group** command to remove a specified NAT-PT address pool.

Note that:

- If *start-ipv4-address* equals *end-ipv4-address*, only one address is available in the address pool.
- The execution of the **undo natpt address-group** command may affect some dynamic NAT-PT mappings.
- Currently, a NAT-PT address pool and an IPv4 NAT address pool do not share any address.
- When there is only one address in the NAT-PT address pool, the address is applied to only NAPT-PT. When there is more than one address in the NAT-PT address pool, the end IPv4 address is reserved for NAPT-PT. The number of addresses applied to dynamic NAT-PT mapping is the number of configured addresses minus 1.

Example # Configure a NAT-PT address pool.

```
<Sysname> system-view
[Sysname] natpt address-group 3 2.3.4.5 2.3.4.10
```

natpt aging-time

Syntax natpt aging-time { default | { dns | finrst | frag | icmp | syn | frag | tcp | udp | } time-value }

View System view

Parameter **default**: Restores the default NAT-PT session timeout time.

dns: Specifies the **DNS** packet timeout time (in seconds), in the range of 5 to 600.

finrst: Specifies the FIN packet timeout time (in seconds), in the range of 5 to 600.

frag: Specifies the FRAG packet timeout time (in seconds), in the range of 5 to 600.

icmp: Specifies the ICMP packet timeout time (in seconds), in the range of 5 to 600.

syn: Specifies the SYN packet timeout time (in seconds), in the range of 5 to 600.

udp: Specifies the UDP packet timeout time (in seconds), in the range of 5 to 600.

tcp: Specifies the TCP packet timeout time (in seconds), in the range of 5 to 86,400.

time-value: NAT-PT session timeout time

Description Use the **natpt aging-time** command to set the NAT-PT session timeout time for different protocol packets.

By default, the timeout time for different protocol packets is as follows:

- 10 seconds for a DNS packet
- 5 seconds for a FINRST packet
- 5 seconds for a FRAG packet
- 20 seconds for an ICMP packet
- 240 seconds for a SYN packet
- 40 seconds for a UDP packet
- 86,400 seconds for a TCP packet

Example # Set the NAT-PT session timeout time to 30 seconds for UDP packets and to 45 seconds for ICMP packets.

```
<Sysname> system-view
[Sysname] natpt aging-time udp 30
[Sysname] natpt aging-time icmp 45
```

natpt enable

Syntax **natpt enable**

undo natpt enable

View Interface view

Parameter None

Description Use the **natpt enable** command to enable the NAT-PT feature on an interface.

Use the **undo natpt enable** command to disable the NAT-PT feature on an interface.

By default, the NAT-PT feature is disabled on an interface. That is, no NAT-PT is implemented for packets received and sent on the interface.

Example # Enable the NAT-PT feature on an interface.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] natpt enable
```

natpt max-session

Syntax **natpt max-session** *max-number*

undo natpt max-session

View System view

Parameter *max-number*: Maximum number of sessions, in the range of 0 to 2,048.

Description Use the **natpt max-session** command to set the maximum number of NAT-PT sessions.

Use the **undo natpt max-session** command to restore the default maximum number of NAT-PT sessions.

By default, the maximum number of NAT-PT sessions is 2,048.

Example # Configure the system to allow 300 concurrent NAT-PT sessions.

```
<Sysname> system-view
[Sysname] natpt max-session 300
```

natpt prefix

Syntax **natpt prefix** *natpt-prefix* [**interface** *interface-type interface-number* [**nexthop** *ipv4-address*]]

undo natpt prefix *natpt-prefix*

View System view

Parameter *natpt-prefix*: Prefix of an IPv6 address, 96 bits in length.

interface-type interface-number: Interface from which an IPv6 packet is forwarded if the prefix of the destination address of the packet complies with the format of the *natpt-prefix* argument during a dynamic mapping on the IPv6 network side.

ipv4-address: IPv4 address of the specified next hop to which an IPv6 packet is forwarded if the prefix of the destination address of the packet complies with the format *natpt-prefix* for a dynamic IPv6-to-IPv4 mapping.

Description Use the **natpt prefix** command to configure the NAT-PT prefix.

Use the **undo natpt prefix** command to remove the configured NAT-PT prefix.

Note that:

- A NAT-PT prefix must be different from an IPv6 address prefix of an interface on the NAT-PT device. Otherwise, the NAT-PT device will implement a NAT-PT after receiving such a packet from an IPv6 node, resulting in packet loss.
- The execution of the **undo natpt prefix** command may affect the translation of some dynamic mappings. Therefore, be careful with this command.

Example # Configure a NAT-PT prefix.

```
<Sysname> system-view
[Sysname] natpt prefix 2001::
```

natpt turn-off tos

Syntax **natpt turn-off tos**

undo natpt turn-off tos

View System view

Parameter None

Description Use the **natpt turn-off tos** command to set the ToS field in an IPv4 packet translated from IPv6 to 0.

Use the **undo natpt turn-off tos** command to set the ToS field in an IPv4 packet translated from an IPv6 packet to the value of the Traffic Class field in the IPv6 packet.

By default, the value of the ToS field in an IPv4 packet translated from an IPv6 packet is the same as that of the Traffic Class field in the IPv6 packet.

Example # Set the ToS field in an IPv4 packet translated from an IPv6 packet to 0.

```
<Sysname> system-view
[Sysname] natpt turn-off tos
```

natpt turn-off traffic-class

Syntax **natpt turn-off traffic-class**

undo natpt turn-off traffic-class

View System view

Parameter None

Description Use the **natpt turn-off traffic-class** command to set the Traffic Class field in an IPv6 packet translated from an IPv4 packet to 0.

Use the **undo natpt turn-off traffic-class** command to set the Traffic Class field in an IPv6 packet translated from an IPv4 packet to the value of the ToS field in the IPv4 packet.

By default, the value of the Traffic Class field in an IPv6 packet translated from an IPv4 packet is the same as that of the ToS field in the IPv4 packet.

Example # Set the Traffic Class field in an IPv6 packet translated from an IPv4 packet to 0.

```
<Sysname> system-view
[Sysname] natpt turn-off traffic-class
```

natpt v4bound dynamic

Syntax **natpt v4bound dynamic acl number** *acl-number* **prefix** *natpt-prefix*

undo natpt v4bound dynamic acl number *acl-number*

View System view

Parameter *acl-number*: IPv4 access control list (ACL) number, in the range of 2000 to 2999.

natpt-prefix: NAT-PT prefix, 96 bits in length.

Description Use the **natpt v4bound dynamic** command to configure a dynamic IPv4-to-IPv6 mapping.

Use the **undo natpt v4bound dynamic** command to remove the dynamic mapping.

For a packet from an IPv4 host to an IPv6 host, if the source IPv4 address complies with the specified ACL rule, a NAT-PT prefix will be added to translate the source IPv4 address into an IPv6 address.

CAUTION: *The natpt-prefix argument in the* ***natpt v4bound dynamic*** *command must be specified by the* ***natpt prefix*** *command in advance.*

Example # Use ACL 2000 to identify the source address of an IPv4 packet and add the NAT-PT prefix 2001:: to translate the source address into an IPv6 address.

```
<Sysname> system-view
[Sysname] natpt prefix 2001::
[Sysname] natpt v4bound dynamic acl number 2000 prefix 2001::
```

natpt v4bound static

Syntax **natpt v4bound static** { *ipv4-address ipv6-address* | **v6server protocol** *protocol-type ipv4-address-destination ipv4-port-number ipv6-address-destination ipv6-port-number* }

undo natpt v4bound static { *ipv4-address ipv6-address* | **v6server protocol** *protocol-type ipv4-address-destination ipv4-port-number ipv6-address-destination ipv6-port-number* }

View System view

Parameter *ipv4-address:* Source IPv4 address to be mapped.

ipv6-address: IPv6 address to which the source IPv4 address is mapped.

v6server: Specifies to implement the protocol-specific port mapping at the time of address mapping.

protocol-type: Protocol type, including TCP and UDP.

ipv4-address-destination: Destination IPv4 address to be mapped.

ipv4-port-number: IPv4 port number, in the range of 1 to 12287.

ipv6-address-destination: IPv6 address to which the destination IPv4 address is mapped

ipv6-port-number: IPv6 port number, in the range of 1 to 12287.

Description Use the **natpt v4bound static** command to configure the static source IPv4-to-IPv6 address mapping or the static destination IPv4-to-IPv6 address/port mapping.

Use the **undo natpt v4bound static** command to remove the static source IPv4-to-IPv6 address mapping or the static destination IPv4-to-IPv6 address/port mapping.

The *ipv6-address* prefix can be different from the NAT-PT prefix, but it is recommended to be the same as the NAT-PT prefix.

Example # Configure the static mapping from the source IPv4 address 2.3.4.9 to the destination IPv6 address 2001::1.

```
<Sysname> system-view
[Sysname] natpt v4bound static 2.3.4.9 2001::1
```

natpt v6bound dynamic

Syntax **natpt v6bound dynamic** { **acl6 number** *acl6-number* | **prefix** *natpt-prefix* } { **address-group** *address-group* [**no-pat**] | **interface** *interface-type interface-number* }

undo natpt v6bound dynamic { **acl6 number** *acl6-number* | **prefix** *natpt-prefix* }

View System view

Parameter *acl-number*: IPv6 access control list (ACL) number, in the range of 2000 to 2999.

natpt-prefix: NAT-PT prefix, 96 bits in length.

address-group: IPv4 address pool number, in the range of 1 to 31.

interface-type: IPv4 interface type.

interface-number: IPv4 interface number.

no-pat: Specifies no port address translation. If the **no-pat** keyword is not provided, port address translation will be performed.

Description Use the **natpt v6bound dynamic** command to configure a dynamic mapping for packets going from an IPv6 node to an IPv4 node.

Use the **undo natpt v6bound dynamic** command to remove the configured dynamic mapping.

Example # Translate the source address of an IPv6 packet that matches IPv6 ACL 2001 into an IPv4 address in address pool 1.

```
<Sysname> system-view
[Sysname] natpt address-group 1 2.3.4.5 2.3.4.10
[Sysname] natpt v6bound dynamic acl6 number 2001 address-group 1
```

natpt v6bound static

Syntax **natpt v6bound static** *ipv6-address ipv4-address*

undo natpt v6bound static *ipv6-address ipv4-address*

View System view

Parameter *ipv6-address*: Source IPv6 address to be mapped.

ipv4-address: IPv4 address to which an IPv6 address is mapped.

Description Use the **natpt v6bound static** command to configure the static IPv6-to-IPv4 address mapping.

Use the **undo natpt v6bound static** command to remove the static IPv6-to-IPv4 address mapping.

Example # Configure the static mapping between the source IPv6 address 2001::1 and the IPv4 address 2.3.4.5.

```
<Sysname> system-view
[Sysname] natpt v6bound static 2001::1 2.3.4.5
```

reset natpt dynamic-mappings

Syntax **reset natpt dynamic-mappings**

View User view

Parameter None

Description Use the **reset natpt dynamic-mappings** command to clear dynamic NAT-PT address mappings.

Example # Clear dynamic NAT-PT address mappings.

```
<Sysname> reset natpt dynamic-mappings
```

reset natpt statistics

Syntax **reset natpt statistics**

View User view

Parameter None

Description Use the **reset natpt statistics** command to clear all NAT-PT statistics information.

Example # Clear all NAT-PT statistics information.

```
<Sysname> reset natpt statistics
```

67 DUAL STACK CONFIGURATION COMMANDS

ipv6

Syntax **ipv6**

undo ipv6

View System view

Parameter None

Description Use the **ipv6** command to enable the IPv6 packet forwarding function.

Use the **undo ipv6** command to disable the IPv6 packet forwarding function.

By default, the function is disabled.

Example # Enable the IPv6 packet forwarding function.

```
<Sysname> system-view
[Sysname] ipv6
```

ipv6 address

Syntax **ipv6 address** { *ipv6-address prefix-length* | *ipv6-address*/*prefix-length* }

undo ipv6 address [*ipv6-address prefix-length* | *ipv6-address*/*prefix-length*]

View Interface view

Parameter *ipv6-address*: IPv6 address for the interface.

prefix-length: Length of the prefix in bits, in the range of 1 to 128.

Description Use the **ipv6 address** command to configure a site-local address or global unicast address for an interface.

Use the **undo ipv6 address** command to remove the configuration.

By default, neither site-local addresses nor global unicast addresses are configured.

Note that:

- Up to 10 global unicast addresses and site-local addresses can be configured on an interface in total.
- The **undo ipv6 address** command without parameters removes all IPv6 addresses manually configured, except link-local addresses automatically configured on the interface.

Example # Set the global unicast address of interface Ethernet 1/1 to 2001::1/64.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ipv6 address 2001::1/64
```

ipv6 address auto link-local

Syntax **ipv6 address auto link-local**

undo ipv6 address auto link-local

View Interface view

Parameter None

Description Use the **ipv6 address auto link-local** command to enable the device to automatically create a link-local address for an interface.

Use the **undo ipv6 address auto link-local** command to remove the automatically created link-local address.

By default, a link-local address will automatically be generated when an IPv6 site-local address or IPv6 global unicast address is configured for an interface.

Example # Enable interface Ethernet 1/1 to create a link-local address automatically.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ipv6 address auto link-local
```

ipv6 address eui-64

Syntax **ipv6 address** *ipv6-address/prefix-length* **eui-64**

undo ipv6 address *ipv6-address/prefix-length* **eui-64**

View Ethernet interface view

Parameter *ipv6-address***/***prefix-length*: IPv6 address and prefix length. They together specify the prefix of an IPv6 address in the EUI-64 format. The prefix length of an EUI-64 address ranges from 1 to 64.

Description Use the **ipv6 address eui-64** command to configure a site-local address or global unicast address in the EUI-64 format on an interface.

Use the **undo ipv6 address eui-64** command to delete the site-local address or global unicast address in the EUI-64 format on an interface.

By default, no site-local or global unicast address in the EUI-64 format is configured for an interface.

Example # Configure Ethernet 1/1 to create an IPv6 address in the EUI-64 format.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ipv6 address 2001::1/64 eui-64
```

ipv6 address link-local

Syntax **ipv6 address** *ipv6-address* **link-local**

undo ipv6 address *ipv6-address* **link-local**

View Interface view

Parameter *ipv6-address*: IPv6 link-local address. The high-order ten bits of an IPv6 link-local address must be 1111111010 (binary), that is to say, the first group of the IPv6 link-local address must range from FE80 to FEBF (hexadecimal).

Description Use the **ipv6 address link-local** command to configure manually a link-local address for the current interface.

Use the **undo ipv6 address link-local** command to remove the link-local address of the interface.

By default, a link-local address will automatically be generated when an IPv6 site-local address or global unicast address is configured for an interface.

Example # Configure a link-local address on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ipv6 address fe80::1 link-local
```

68 TUNNELING CONFIGURATION COMMANDS

A tunnel interface number is in the X format, where X ranges from 0 to 1023.

destination

Syntax **destination** { *ip-address* | *ipv6-address* }

undo destination

View Tunnel interface view

Parameter *ip-address*: Destination IPv4 address of a specified tunnel interface.

ip-address: Destination IPv6 address of a specified tunnel interface.

Description Use the command **destination** to specify a destination address for the tunnel interface.

Use the **undo destination** command to remove the configured destination IP address.

By default, no destination address is configured for the tunnel interface.

Note that:

- The destination address of a tunnel interface is the address of the peer interface receiving packets and is usually the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source and destination addresses.

Related command: **interface tunnel** and **source**.

Example # Set Serial2/0 (193.101.1.1) of Sysname 1 and Serial2/0 (192.100.1.1) of Sysname 2 to the source and destination interfaces of a tunnel between two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface tunnel 0
[Sysname1-Tunnel0] source 193.101.1.1
[Sysname1-Tunnel0] destination 192.100.1.1
<Sysname2> system-view
```

```
[Sysname2] interface tunnel 1
[Sysname2-Tunnel1] source 192.100.1.1
[Sysname2-Tunnel1] destination 193.101.1.1
```

display interface tunnel

Syntax **display interface tunnel** [*number*]

View Any view

Parameter *number*: Tunnel interface number. If the *number* argument is not specified, the information of all tunnel interfaces will be displayed.

Description Use the **display interface tunnel** command to display related information of a specified tunnel interface, such as source address, destination address, and encapsulation mode.

Related command: **interface tunnel**, **source**, **destination**, and **tunnel-protocol**.

Example # Display information of the interface tunnel 0.

```
<Sysname> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, aggregation ID not set
Tunnel source 192.13.2.1, destination 192.13.2.2
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP
    GRE key disabled
    Checksumming of GRE packets disabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    361 packets input,  9953388 bytes
    0 input error
    361 packets output,  30324 bytes
    0 output error
```

Table 189 Description on fields of the display interface tunnel command

Field	Description
Tunnel0 current state: UP	The physical layer of the tunnel interface is reachable.
Line protocol current state: UP	The link layer of the tunnel interface is reachable.
Description	Descriptive information of a tunnel interface
Tunnel0 Interface	Tunnel interface number
Maximum Transmit Unit	Maximum transmission unit (MTU) in a tunnel
Encapsulation is TUNNEL	The encapsulation protocol is tunnel.

Table 189 Description on fields of the display interface tunnel command

Field	Description
aggregation ID	Link aggregation group ID referenced by a tunnel. If the device supports link aggregation groups, the link aggregation group ID configured in tunnel interface view is displayed. If device does not support, "aggregation ID not set" is displayed.
Tunnel source	Source address of a tunnel.
destination	Destination address of a tunnel.
Tunnel keepalive disable	Disables the keepalive function of the GRE so as not to detect the tunnel interface state.
Tunnel protocol/transport	Tunnel protocol and transport protocol.
GRE key disabled	No key is configured for the GRE tunnel interface.
Checksumming of GRE packets disabled	Disables the GRE packet checksum function.
Last 300 seconds input	Number of bytes and packets input per second in the last five minutes.
Last 300 seconds output	Number of bytes and packets output per second in the last five minutes.
packets input	Total number of input packets.
input error	Number of error packets among all input packets.
packets output	Total number of output packets.
output error	Number of error packets in all output packets

display ipv6 interface tunnel

Syntax **display ipv6 interface tunnel** *number*

View Any view

Parameter *number*: Tunnel interface number.

Description Use the **display ipv6 interface tunnel** command to display related IPv6 information of a specified tunnel interface, including link state, IPv6 protocol state, and IPv6 address.

Example # Display information of the interface tunnel 0.

```
<Sysname> display ipv6 interface tunnel 0
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::101:101
  Global unicast address(es):
    2002:101:101::1, subnet is 2002::/16
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
```

```
ND reachable time is 30000 milliseconds
ND retransmit interval is 1000 milliseconds
Hosts use stateless autoconfig for addresses
```

Table 190 Description on fields of the display interface tunnel command

Field	Description
Tunnel0 current state: UP	The physical layer of the tunnel interface is reachable.
Line protocol current state: UP	The link layer of the tunnel interface is reachable.
IPv6 is enabled	Enables IPv6 on a tunnel interface
link-local address	Link-local address of a tunnel interface
Global unicast address(es)	Aggregatable global unicast address of a tunnel interface.
Joined group address(es)	Multicast address of a tunnel interface.
MTU is 1500 bytes	Size of the MTU in a tunnel. The MTU in this example is 1,500 bytes.
ND reachable time	Neighbor reachable time
ND retransmit interval	Interval for retransmitting a neighbor discovery message.
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire IPv6 addresses.

encapsulation-limit

Syntax **encapsulation-limit** [*number*]

undo encapsulation-limit

View Tunnel interface view

Parameter *number*: Number of nested encapsulations in a tunnel, in the range of 1 to 10. The default value is 4.

Description Use the **encapsulation-limit** command to configure the maximum number of nested encapsulations of a packet.

Use the **undo encapsulation-limit** command to remove the encapsulation limit.

The encapsulation limit is only applicable to the IPv6 over IPv6 tunnel.

Example # Configure the maximum number of nested encapsulations in a tunnel to 3.

```
<Sysname> system-view
[Sysname] interface tunnel 2
[Sysname-Tunnel2] tunnel-protocol ipv6-ipv6
[Sysname-Tunnel2] encapsulation-limit 3
```

interface tunnel

Syntax **interface tunnel** *number*

undo interface tunnel *number*

View System view

Parameter *number*: Tunnel interface number, in the range of 0 to 1023. The number of tunnels that can be created is restricted by the total number of interfaces and the memory.

Description Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove a specified tunnel interface.

By default, there is no tunnel interface on the device.

- Carry out the **interface tunnel** command to enter interface view of a specified tunnel. If the tunnel interface is not created, you must create it before entering tunnel interface view.
- A tunnel interface number has only local significance, and therefore, the same interface number or different interface numbers can be set at both ends of a tunnel.

Related command: **display interface tunnel**, **source**, **destination**, and **tunnel-protocol**.

Example # Create the interface tunnel 3.

```
<Sysname> system-view
[Sysname] interface tunnel 3
[Sysname-Tunnel3]
```

mtu

Syntax **mtu** *mtu-size*

undo mtu

View Tunnel interface view

Parameter *mtu-size*: Tunnel interface MTU in bytes, in the range of 100 to 64,000.

Description Use the **mtu** command to configure the tunnel interface MTU.

Use the **undo mtu** command to restore the default tunnel interface MTU.

The default value varies with devices.

Example # Set the tunnel interface MTU to 10,000 bytes.

```
<Sysname> system-view
[Sysname] interface tunnel 3
[Sysname-Tunnel3] mtu 10000
```

source

Syntax **source** { *ip-address* | *ipv6-address* | *interface-type interface-num* }

undo source

View Tunnel interface view

Parameter *ip-address*: Source IPv4 address of a tunnel interface.

ip-address: Source IPv6 address of a tunnel interface.

interface-type interface-number: Specifies an interface. The interface types include Ethernet, serial, ATM, tunnel, and loopback.

Description Use the **source** command to specify a source address for a tunnel interface.

Use the **undo source** command to remove the configured source IP address.

By default, no source address is configured for a tunnel interface.

Note that:

- The source address of a tunnel interface is the address of the interface sending packets and is usually the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related command: **interface tunnel** and **destination**.

Example # Configure the interface tunnel 5. The actual outgoing interface encapsulating packets is Serial2/0 (192.100.1.1).

```
<Sysname> system-view
[Sysname] interface tunnel 5
[Sysname-Tunnel5] source 192.100.1.1
```

Or

```
<Sysname> system-view
[Sysname] interface tunnel 5
[Sysname-Tunnel5] source serial 2/0
```

tunnel-protocol

Syntax **tunnel-protocol** { **ipv4-ipv4** | **ipv6-ipv4** [**6to4** | **auto-tunnel** | **isatap**] | **ipv6-ipv6** | **ipv4-ipv6** }

undo tunnel-protocol

View Tunnel interface view

Parameter **ipv4-ipv4**: Sets the tunnel to an IPv4 over IPv4 tunnel.

Ipv4-ipv6: Sets the tunnel to an IPv4 over IPv6 tunnel.

ipv6-ipv4: Sets the tunnel to an IPv6 over IPv4 tunnel.

ipv6-ipv4 6to4: Sets the tunnel to IPv6 over IPv4 6to4 tunnel.

ipv6-ipv4 auto-tunnel: Sets the tunnel to an automatic IPv4 compatible IPv6 tunnel.

ipv6-ipv4 isatap: Sets the tunnel to an IPv6 over IPv4 ISATAP tunnel.

ipv6-ipv6: Sets the tunnel to an IPv6 over IPv6 tunnel.

mpls te: Sets the tunnel to an MPLS TE tunnel.

Description Use the **tunnel-protocol** command to configure the tunnel type.

Use the **undo tunnel-protocol** to restore the tunnel type to the default.

By default, the tunnel is GRE tunnel.

Note that:

- A proper tunnel type can be selected for packet encapsulation according to the network topology and application. The same tunnel type must be configured at both ends of the tunnel. Otherwise, packet delivery will fail.
- Only one automatic tunnel can be configured at the same tunnel source.

For details about MPLS TE tunnel, refer to "mpls te tunnel-id" on page 1636.

Example # Specify the tunnel type as IPv4 over IPv4 for a tunnel interface.

```
<Sysname> system-view
[Sysname] interface tunnel 2
[Sysname-Tunnel2] tunnel-protocol ipv4-ipv4
```

69 IPv6 Unicast Policy Routing Configuration Commands

apply default output-interface

Syntax **apply default output-interface** *interface-type interface-number*

undo apply default output-interface [*interface-type interface-number*]

View IPv6 policy-based-route view

Parameter *interface-type interface-number*: Specifies an interface.

Description Use the **apply default output-interface** command to set a default outgoing interface for IPv6 packets.

Use the **undo apply default output-interface** command to remove the default outgoing interface.

This command only applies to packets not finding a match in the routing table. You can specify up to five default outgoing interfaces, implementing load balancing based on data streams.

Related command: **apply ipv6-precedence**, **apply ipv6-address next-hop**, **apply output-interface**, **apply ipv6-address default next-hop**.

Example # Set the default outgoing interface to the interface Serial 2/0.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply default output-interface serial 2/0
```

apply destination-based-forwarding

Syntax **apply destination-based-forwarding**

undo apply destination-based-forwarding

View IPv6 policy-based-route view

Parameter None

Description Use the **apply destination-based-forwarding** command to enable destination based forwarding.

Use the **undo apply destination-based-forwarding** command to disable destination based forwarding.

By default, destination based forwarding is disabled.

With destination based forwarding enabled, IPv6 packets not matching the policy node can be routed through the routing table; otherwise, such packets will be discarded.

Example # Enable destination based forwarding.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply destination-based-forwarding
```

apply ipv6-address default next-hop

Syntax **apply ipv6-address default next-hop** *ipv6-address*

undo apply ipv6-address default next-hop [*ipv6-address*]

View IPv6 policy-based-route view

Parameter *ipv6-address*: Default next hop.

Description Use the **apply ipv6-address default next-hop** command to set a default next hop for matched IPv6 packets.

Use the **undo apply ipv6-address default next-hop** command to remove the default next hop.

This command only applies to packets not finding a match in the routing table. You can specify up to five default next hops, implementing load balancing based on data streams. The interface to reach the next hop must be a P2P interface rather than a broadcast interface.

Related command: **apply ipv6-precedence**, **apply output-interface**, **apply default output-interface** and **apply ipv6-address next-hop**.

Example # Set a default next hop of 1::1 for matched IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply ipv6-address default next-hop 1::1
```

apply ipv6-address next-hop

Syntax **apply ipv6-address next-hop** *ipv6-address*

undo apply ipv6-address next-hop [*ipv6-address*]

View IPv6 policy-based-route view

Parameter *ipv6-address*: IPv6 address of a next hop

Description Use the **apply ipv6-address next-hop** command to set a next hop for matched IPv6 packets.

Use the **undo apply ipv6-address next-hop** command to remove the next hop.

The next hop must be adjacent to the device. You can specify up to five next hops, implementing load balancing based on data streams.

Related command: **apply ipv6-precedence**, **apply output-interface**, **apply default output-interface** and **apply ipv6-address default next-hop**.

Example # Set a next hop of 1::1 for matched IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply ipv6-address next-hop 1::1
```

apply ipv6-precedence

Syntax **apply ipv6-precedence** { *type* | *value* }

undo apply ipv6-precedence

View IPv6 policy-based-route view

Parameter *type*: Preference type for matched IPv6 packets, types including routine, priority, immediate, flash, flash-override, critical internet and network.

value: Preference value for matched IPv6 packets from 0 to 7 (inclusive). Each value corresponds to a keyword, as shown in the following table.

Table 191 Preferences and the corresponding keywords

Preference value	Keyword
0	routine
1	priority
2	immediate
3	flash

Table 191 Preferences and the corresponding keywords

Preference value	Keyword
4	flash-override
5	critical
6	internet
7	network

Description Use the **apply ipv6-precedence** command to set a preference for matched IPv6 packets.

Use the **undo apply ipv6-precedence** command to remove the preference.

Related command: **apply output-interface**, **apply ipv6-address next-hop**, **apply default output-interface**, **apply ipv6-address default next-hop**.

Example # Set a preference of 5 (critical) for matched IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply ipv6-precedence critical
```

apply output-interface

Syntax **apply output-interface** *interface-type interface-number*

undo apply output-interface [*interface-type interface-number*]

View IPv6 policy-based-route view

Parameter *interface-type interface-number*: Specifies an interface.

Description Use the **apply output-interface** command to set an outgoing interface for matched IPv6 packets.

Use the **undo apply output-interface** command to remove the outgoing interface.

Note that:

- Five outgoing interfaces at most can be specified, and load balancing based on data streams can be implemented.
- For non-P2P interfaces (broadcast and NBMA interfaces) such as Ethernet interface, multiple next hops are available, and thus packets may not be forwarded successfully.

Related command: **apply ipv6-precedence**, **apply ipv6-address next-hop**, **apply default output-interface**, **apply ipv6-address default next-hop**.

Example # Specify the interface Serial 2/0 as the outgoing interface for matched IPv6 packets.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] apply output-interface serial 2/0
```

display ipv6 config policy-based-route

Syntax **display ipv6 config policy-based-route** *policy-name*

View Any view

Parameter *policy-name*: Policy name, a string of 1 to 19 characters.

Description Use the **display ipv6 config policy-based-route** command to display the configured IPv6 policy routing information.

Example # Display the configured IPv6 policy routing information.

```
<Sysname> display ipv6 config policy-based-route
 IPv6 Policy based routing configuration information:
 ipv6 policy-based-route : abc
  Node  1  permit :
       apply output-interface Ethernet1/0
```

Table 192 Description on the fields of the display ipv6 config policy-based-route command

Field	Description
IPv6 Policy based routing configuration information	IPv6 policy routing configuration information
ipv6 policy-based-route: abc	Policy name
Node 1 permit :	The match mode of Node 1 is permit.
apply output-interface Ethernet1/0	The outgoing interface for matched packet is Ethernet1/0.

display ipv6 policy-based-route

Syntax **display ipv6 policy-based-route**

View Any view

Parameter None

Description Use the **display ipv6 policy-based-route** command to display system and interface IPv6 policy routing information.

Example # Display system and interface IPv6 policy routing information.

```
<Sysname> display ipv6 policy-based-route
Policy Name              interface
pr02                     local
pr02                     Virtual-Template0
pr01                     Ethernet 1/0
```

Table 193 Description on fields of the display ipv6 policy-based-route command

Field	Description
Local	System policy routing
pr02	Policy name
Virtual-Template0	Policy pr02 applied to Virtual-template0
Ethernet1/0	Policy pr01 applied to Ethernet1/0

display ipv6 policy-based-route setup

Syntax **display ipv6 policy-based-route setup** { *policy-name* | **interface** *interface-type interface-number* | **local** }

View Any view

Parameter *policy-name*: Policy name, a string of 1 to 19 characters.

interface *interface-type interface-number*: Displays policy routing information on the specified interface.

local: Displays system policy routing information.

Description Use the **display ipv6 policy-based-route setup** command to display specified IPv6 policy routing configuration information.

Example # Display specified IPv6 policy routing configuration information.

```
<Sysname> display ipv6 policy-based-route setup local
Local policy based routing configuration information:
ipv6 policy-based-route : test
  Node  6  permit :
    if-match acl6 2000
  Node  10  permit :
    apply destination-based-forwarding
```

Table 194 Description on fields of the display ipv6 policy-based-route setup command

Field	Description
ipv6 policy-based-route : test	Name of the referenced policy
Node 6 permit	The match mode of Node 6 is permit.
if-match acl6 2000	IPv6 packets matching IPv6 ACL 2000 are permitted.
Node 10 permit	The match mode of Node 10 is permit.
apply destination-based-forwarding	Enable destination based forwarding for denied IPv6 packets

display ipv6 policy-based-route statistics

Syntax **display ipv6 policy-based-route statistics** { **interface** *interface-type interface-number* | **local** }

View Any view

Parameter **interface** *interface-type interface-number*: Displays IPv6 policy routing statistics on the specified interface.

local: Displays IPv6 system policy routing statistics.

Description Use the **display ipv6 policy-based-route statistics** command to display IPv6 policy routing statistics.

Example # Display IPv6 system policy routing statistics.

```
<Sysname> display ipv6 policy-based-route statistics local
Local policy based routing information:
  ipv6 policy-based-route: test
  permit node 10
  Total packet dropped at node level: 0
 Total packet denied: 0, forwarded: 0
```

Table 195 Description on fields of the display ipv6 policy-based-route statistics command

Field	Description
Local policy based routing information	System policy routing information
ipv6 policy-based-route: test	Name of the referenced policy
Total packet dropped at node level: 0	Packets dropped by the node
Total packet denied: 0, forwarded: 0	Packets denied by the policy and packets forwarded by the policy

if-match acl6

Syntax **if-match acl6** *acl6-number*

undo if-match acl6

View IPv6 policy-based-route view

Parameter *acl6-number*: IPv6 ACL number, in the range 2000 to 3999. The number of a basic IPv6 ACL ranges from 2000 to 2999 and that of an advanced IPv6 ACL ranges from 3000 to 3999.

Description Use the **if-match acl6** command to define an IPv6 ACL match rule.

Use the **undo if-match acl6** command to remove the IPv6 ACL match rule.

Related command: **if-match packet-length**.

Example # Permit the packets matching ACL 2000.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 10
[Sysname-pbr6-aa-10] if-match acl6 2000
```

if-match packet-length

Syntax **if-match packet-length** *min-len max-len*

undo if-match packet-length

View IPv6 policy-based-route view

Parameter *min-len*: Minimum IPv6 packet length in bytes, in the range of 0 to 65535.

max-len: Maximum IPv6 packet length in bytes, in the range of 1 to 65535. The value of *max-len* must be no less than that of *min-len*.

Description Use the **if-match packet-length** command to define a packet length match rule.

Use the **undo if-match packet-length** command to remove the match rule.

Related command: **if-match acl6**.

Example # Match the IPv6 packets with a length from 100 to 200 bytes.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aa permit node 11
[Sysname-pbr6-aa-11] if-match packet-length 100 200
```

ipv6 local policy-based-route

Syntax **ipv6 local policy-based-route** *policy-name*

undo ipv6 local policy-based-route [*policy-name*]

View System view

Parameter *policy-name*: Policy name, which uniquely identifies an IPv6 policy routing. It is a string of 1 to 19 characters.

Description Use the **ipv6 local policy-based-route** command to enable IPv6 system policy routing and reference a policy.

Use the **undo ipv6 local policy-based-route** command to disable IPv6 system policy routing.

IPv6 system policy routing is disabled by default.

System policy routing is used to route packets generated locally. Unless otherwise required, you are not recommended to enable system policy routing.

Related command: **ipv6 local policy-based-route**.

Example # Enable IPv6 system policy routing and reference a policy named AAA.

```
<Sysname> system-view
[Sysname] ipv6 local policy-based-route AAA
```

ipv6 policy-based-route (interface view)

Syntax **ipv6 policy-based-route** *policy-name*

undo ipv6 policy-based-route

View Interface view

Parameter *policy-name*: Policy name, which uniquely identifies an IPv6 policy routing. It is a string of 1 to 19 characters.

Description Use the **ipv6 policy-based-route** command to enable IPv6 policy routing and reference a policy on the interface.

Use the **undo ipv6 policy-based-route** command to disable interface policy routing.

IPv6 interface policy routing is disabled by default.

Related command: **ipv6 local policy-based-route**.

Example # Enable IPv6 policy routing and reference a policy named AAA on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 policy-based-route AAA
```

ipv6 policy-based-route (system view)

Syntax **ipv6 policy-based-route** *policy-name* [**deny** | **permit**] **node** *node-number*

undo ipv6 policy-based-route *policy-name* [**deny** | **node** *node-number* | **permit**]

View System view

Parameter *policy-name*: Policy name, a string of 1 to 19 characters.

deny: Specifies the match mode of the policy node as **deny**. When a packet satisfies all rules defined by the **if-match** clauses, the packet will be denied by the

node and will not match against the next policy node. If not, the packet will match against the next policy node.

permit: Specifies the match mode of the policy node as **permit**. If a packet satisfies all the rules defined by the **if-match** clauses, the **apply** clauses are executed. If not, the packet will match against the next policy node.

node *node-number*: Number of the IPv6 policy node, in the range 0 to 65535. Packets will match against the node with a smaller *node-number* first.

Description Use the **ipv6 policy-based-route** command to create an IPv6 policy or policy node and enter IPv6 policy routing view.

Use the **undo ipv6 policy-based-route** command to remove an IPv6 policy or policy node.

No IPv6 policy or policy node is created by default.

An IPv6 policy may consist of several nodes, and a node consists of **if-match** clauses and **apply** clauses. The **if-match** clauses define the match rules for the node and the **apply** clauses define the actions that should be taken for matched packets.

Note that:

- There is an AND relationship between the **if-match** clauses of a node. That is to say, a packet must satisfy all matching rules specified by all **if match** clauses for the node before the action specified by the **apply** clause is taken.
- There is an OR relationship between nodes of the policy. That is, if a packet passes a node, it passes the policy.
- A packet passing a node of a policy will not go to the next node of the policy for a match.
- A packet not passing any node of a policy cannot pass the policy. It will be routed through the routing table.
- If multiple nodes are defined for a policy, the match mode of at least one node must be **permit**.

Related command: **ipv6 local policy-based-route**, **ipv6 local policy-based-route**, **if-match acl6**, **if-match packet-length**.

Example # Create Node 10 for the IPv6 policy "aaa" with match mode being permit and enter IPv6 policy routing view.

```
<Sysname> system-view
[Sysname] ipv6 policy-based-route aaa permit node 10
[Sysname-pbr6-aaa-10]
```

70 TERMINAL ACCESS CONFIGURATION COMMANDS

auto-close

Syntax **auto-close** *time*

undo auto-close

View Terminal template view

Parameters *time*: Automatic link teardown time, in seconds. It ranges from 5 to 240.

Description Use the **auto-close** command to configure the automatic link teardown time.

Use the **undo auto-close** command to restore the default. By default; the automatic link teardown time is 0 seconds, namely, no automatic link teardown is performed.

The terminal access feature supports the automatic link teardown function. You can enable the function and configure the teardown time in terminal template view. With this function enabled, if a terminal is disconnected from the router, the terminal enters the state of DOWN, and the router will automatically tear down the TCP connection to the front-end processor (FEP) after the specified time period. If the function is disabled, the TCP connection will always remain.

Example # Set the automatic link teardown time to 10 seconds.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] auto-close 10
```

auto-link

Syntax **auto-link** *time*

undo auto-link

View Terminal template view

Parameters *time*: Automatic link establishment time, in seconds. It ranges from 5 to 240.

Description Use the **auto-link** command to configure the automatic link establishment time.

Use the **undo auto-link** command to restore the default. By default, the automatic link establishment time is 0 seconds, namely, no automatic link establishment is performed.

The terminal access feature supports the automatic link establishment function. You can enable the function and configure the automatic link establishment time in terminal template view. When the terminal is in the "OK" state (meaning the physical connection is normal), the router automatically establishes a TCP connection to the remote router or FEP after the specified period of time. If the automatic link establishment function is disabled on the terminal, a link needs to established manually (manual link establishment is the default mode). The router establishes a TCP connection to the FEP only after a user enters a character on the terminal, except the special characters for hotkeys and terminals. Special characters are the characters that the terminals process directly, such as <Shift+F2>. For details, see the related manuals of terminals.

Example # Set the automatic link establishment time to 10 seconds.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] auto-link 10
```

bind vpn-instance

Syntax **bind vpn-instance** *vpn-name*

undo bind vpn-instance

View Terminal template view

Parameters *vpn-name*: VPN instance name, a string of 1 to 31 case-insensitive characters.

Description Use the **bind vpn-instance** command to bind a VPN instance with the terminal template. Use the **undo bind vpn-instance** command to remove the VPN instance binding.

By default, no VPN instance is bound with a terminal template.

This configuration is required when the TTY terminal access initiator also acts as an MPLS provider edge (PE) router at the same time. When you apply a terminal template configured with the **bind vpn-instance** command to an asynchronous interface, the terminal corresponding to the asynchronous interface is bound with the VPN instance. Thus, the terminal access initiator can group the terminals into different VPN domains. The RTC server can receive the connection request from any VPN without being configured with the **bind vpn-instance** command.

A template can be bound with only one VPN instance. If VPN instance binding is configured with this command for more than once, the latest configuration applies.

Example # Bind the VPN instance vpn1 with the terminal template.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] bind vpn-instance vpn1
```

data protect router-unix

Syntax **data protect router-unix**

undo data protect router-unix

View Terminal template view

Parameters None

Description Use the **data protect router-unix** command to enable data encryption between the router and the FEP.

Use the **undo data protect** command to restore the default.

By default, data encryption is disabled between the router and the FEP.

In terminal access, you can configure whether to encrypt the data exchanged between the router and the FEP. The supported encryption algorithm is AES (advanced encryption standard) and the supported key length is 128-bit.

Example # Enable the data encryption between the router and the FEP.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] data protect router-unix
```

data read block

Syntax **data read block**

undo data read block

View Terminal template view

Parameters None

Description Use the **data read block** command to enable data read blocking.

Use the **undo data read block** command to restore the default.

By default, data read blocking is disabled.

Note that, if data read blocking is enabled, when the router fails to send data from the terminal, the router stops receiving data from the terminal until the data is sent successfully.

Example # Enable data read blocking.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] data read block
```

data send delay

Syntax **data send delay** *milliseconds*

undo data send delay

View Terminal template view

Parameters *milliseconds*: Data send delay, in *milliseconds, ranging* 1 to 1,000.

Description Use the **data send delay** command to set the data send delay of the terminal.

Use the **undo data send delay** command to restore the default.

By default; the data send delay is 0 milliseconds, namely, there is no data send delay.

A router configured with data send delay begins to send the data received from a terminal to an FEP after the configured data send delay time expires.

Example # Set the data send delay time to 50 milliseconds.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] data send delay 50
```

display rta

Syntax **display rta** { **all** | **statistics** | *terminal-number* { **brief** | **detail** | **statistics** | *vty-number* } }

View Any view

Parameters **all**: Displays information about all the terminals.

statistics: Displays terminal statistics.

terminal-number: Terminal number, ranging 1 to 255.

brief: Displays brief information about the specified terminal.

detail: Displays detailed information about the specified terminal.

vty-number: Displays information about the specified VTY. VTY number ranges from 0 to 7.

Description Use the **display rta** command to display information about terminals.

Relate command: **reset rta statistics**.

Example # Display the information about the terminal VTY1.

```
<Sysname> display rta 1 1
VTY 1
    APP Index: 0
    APP Type: TTY
    APP Name: (null)
    APP State: Kept
    Remote IP: 192.168.0.110
    Source IP: 0.0.0.0
    Actual Source IP: 0.0.0.0
    Remote Port: 9010
    Local Port: 0
    Encrypt Now: no
    Receive remote buffer address: 593c904
    Receive buffer head: 499
    Receive buffer tail: 499
    Time from APP is linked till now: 00h00m00s
```

Table 196 Description on the fields of the display rta terminal-number vty-number command

Field	Description
APP Index	Application index
APP Type	Application type: TTY, Telnet, RTC client, or RTC server
APP Name	Application name. It defaults to "null".
APP State	Application state: Kept, Linking, Linked, Disconnect, meaning respectively not connected, being connected, connected, disconnected.
Remote IP	Remote IP address
Source IP	Source IP address, namely, the source IP address configured for the VTY under the terminal template
Actual Source IP	Actual source IP address, namely, the source IP address used for establishing a connection. This field applies only when the global source IP address for terminal access is configured or when the source IP address is configured for the VTY under the terminal template. In any other cases, it is 0.0.0.0.
Remote Port	Remote port
Local Port	Local port
Encrypt Now	Whether to encrypt data
Receive remote buffer address	Buffer address for receiving remote data
Receive buffer head	Receive buffer head
Receive buffer tail	Receive buffer tail
Time from APP is linked till now	Time since the application was connected

Display brief information about TTY 1.

```
<Sysname> display rta 1 brief
TTY 1
```

```
Interface Used         :  Async1/0
Current State          :  Ok
Flow Control           :  Stop
Current Debug          :  0x3c
Current VTY            :  0
Current APP            :  0
APP Type               :  TTY
  APP Name               :  <empty>
  APP State              :  Kept
Socket RecvBuf Size    :  2048 Bytes
Socket SendBuf Size    :  2048 Bytes
TTY Recv Bytes         :  1371 Bytes
TTY Send Bytes         :  63696 Bytes
Last Recv Time         :  19:39:33
Last Send Time         :  03:39:34
Current VTY Recv       :  1371 Bytes
Current VTY Send       :  63696 Bytes
Current APP Recv       :  55280 Bytes
Current APP Send       :  1524 Bytes
Time from APP is linked: 00h00m00s
Encrypt(Router to Unix): no
Receive remote buffer address: 593c904
Receive buffer head: 2032
Receive buffer tail: 2032
-----------------------------------
VTY       APP       Type       State
0         0         TTY        Kept
```

Table 197 Description on the fields of the display rta terminal-number brief command

Field	Description
TTY 1	TTY" indicates the terminal access type and "1" the terminal number.
Interface Used	Physical interface corresponding to the terminal number
Current State	Current terminal state: Down, OK, and Menu, respectively meaning physical connection down, physical connection normal, and menu state.
Flow Control	Flow control for the current application: Start or Stop, meaning starting not to receive data from the FEP or starting to receive data from the FEP
Current Debug	Whether current debugging is enabled or disabled
Current VTY	Currently operating VTY
Current APP	Current application
APP Type	Application type
APP Name	Application name
APP State	Application state
Socket RecvBuf Size	TCP receive buffer size
Socket SendBuf Size	TCP send buffer size
TTY Recv Bytes	Received data in bytes
TTY Send Bytes	Transmitted data in bytes
Last Recv Time	Time when last data was received
Last Send Time	Time when last data was sent
Current VTY Recv	Data, in bytes, received by the current VTY

Table 197 Description on the fields of the display rta terminal-number brief command

Field	Description
Current VTY Send	Data, in bytes, sent by the current VTY
Current APP Recv	Data, in bytes, received by the current application
Current APP Send	Data, in bytes, sent by the current application
Time from APP is linked	Time since the application was connected
Encrypt(Router to Unix)	Whether to encrypt data
Receive Remote Buffer Address	Buffer address for receiving remote data
Receive Buffer Tail	Receive buffer head
Receive Buffer Tail	Receive buffer tail
VTY APP Type State	VTY list configured on the terminal. "VTY" represents VTY number; "APP" represents application; "Type" represents application type; "State" represents application state.

Display statistics about terminal 1.

```
<Sysname> display rta 1 statistics
TTY 1
  Receive from terminal: 0
  Send to terminal:      0
  Receive from remote:   0
  Send to remote:        0

  VTY 0
    Receive from terminal: 0              Last receive time: 00:00:00
    Send to terminal:      0              Last send time:    00:00:00
    Receive from remote:   0              Last receive time: 00:00:00
    Send to remote:        0              Last send time:    00:00:00
```

Table 198 Description on the fields of the display rta terminal-number statistics command

Field	Description
Receive from terminal	Data, in bytes, received from the terminal
Send to terminal	Data, in bytes, sent to the terminal
Receive from remote	Data, in bytes, received from the remote terminal
Send to remote	Data, in bytes, sent to the remote terminal
Last receive time	Time when last data was received
Last send time	Time when last data was sent

Display all the information about terminal access.

```
<Sysname> display rta all
TTYID    TTY State    Current VTY    Current APP    APP Type    APP State
1        OK           0              0              TTY         Kept
```

Table 199 Description on the fields of the display rta all command

Field	Description
TTYID	Terminal number
TTY State	Terminal state
Current VTY	VTY currently operating on the terminal
Current APP	Current application
APP Type	Application type

Table 199 Description on the fields of the display rta all command

Field	Description
APP State	Application state

Display terminal access statistics

```
<Sysname> display rta statistics
    RTA Template Number: 2
    RTA TTY Number: 1
    RTA APP Number: 1
    RTA Listen Port Number: 0
```

Table 200 Description on the fields of the display rta statistics command

Field	Description
RTA Template Number	Number of terminal templates configured on the router
RTA TTY Number	Number of terminals configured on the router
RTA APP Number	Number of applications generated after terminal configuration
RTA Listen Port Number	Number of listening ports on the router

driverbuf save

Syntax **driverbuf save**

undo driverbuf save

View Terminal template view

Parameters None

Description Use the **driverbuf save** command to configure the router not to clear the terminal receive buffer after the TCP connection is established

Use the **undo driverbuf save** command to restore the default.

By default, the router clears the terminal receive buffer after the TCP connection is established.

Terminal receive buffer is the buffer used on a router to store terminal data.

Example # Configure not to clear the terminal receive buffer after the TCP connection is established

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] driverbuf save
```

driverbuf size

Syntax **driverbuf size** *number*

undo driverbuf size

View Terminal template view

Parameters *number*: Buffer size, in kilobytes (KB), ranging from 8 to 32.

Description Use the **driverbuf size** command to configure the size of terminal receive buffer.

Use the **undo driverbuf size** command to restore the default setting.

By default, the size of terminal receiver buffer is 8 KB.

Note that this command takes effect only after the template is reapplied on the interface.

Example # Set the terminal buffer size to 8 KB.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] driverbuf size 8
```

idle-timeout

Syntax **idle-timeout** *seconds*

undo idle-timeout

View Terminal template view

Parameters *seconds*: Connection idle timeout time, in seconds, ranging 10 to 3,600.

Description Use the **idle-timeout** command to set the TCP connection idle timeout time for terminal access.

Use the **undo idle-timeout** command to restore the default.

By default, the terminal access idle timeout time is 0 seconds; that is, the TCP connection never times out.

With the idle timeout time configured, if no data is transmitted over the terminal access connection in the specified period of time, the connection is automatically torn down.

Example # Set the terminal access idle timeout time to 1,000 seconds.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] idle-timeout 1000
```

menu hotkey

Syntax **menu hotkey** *ascii-code*&<1-3>

undo menu hotkey

View Terminal template view

Parameters *ascii-code*&<1-3>: ASCII value of hotkey, ranging 1 to 255. "&<1-3>" means that you can provide up to three hotkey ASCII values.

Description Use the **menu hotkey** command to configure the menu hotkey.

Use the **undo menu hotkey** command to cancel the menu hotkey configured.

By default, no menu hotkey is configured.

If the current terminal operates on the service interface, you can switch to the menu interface by entering the menu hotkey configured.

RTC terminal access does not support the menu function.

Note:

- The ASCII value of the hotkey must be different from that of any other hotkey configured on the device. Otherwise, hotkey conflicts will occur. For example, the hotkey value cannot be set to 17 or 19 because these two values are used for the hotkeys of flow control.
- Using the hotkey may not get a response rapidly when the terminal displays too much data.
- Before using this command, make sure you enable the router to print characters to the terminal and enable menu printing.

Related command: **print information** and **print menu**.

Example # Configure the hotkey for switching to the menu as <Alt+A>, whose corresponding ASCII codes are a combination of 1, 96, and 13.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] menu hotkey 1 96 13
```

menu screencode

Syntax **menu screencode** *string*

undo menu screencode

View Terminal template view

Parameters *string*: Screen code of the terminal, containing 1 to 15 case-insensitive characters.

Description Use the **menu screencode** command to configure a menu screen code.

Use the **undo menu screencode** command to remove the menu screen code.

By default, no such a screen code is configured.

Some types of terminals provide the screen saving function. When such a terminal receives a specific screen code, such as E!10Q (for details about screen codes, refer to the related terminal manuals), it saves the current interface and switch to the corresponding screen.

Note that this function requires terminal support and the screen code configured on the router and that specified on the terminal must be the same. Screen codes vary with terminal types. For details, refer to the corresponding terminal manuals. For example, Start terminals support E!8Q, E!9Q, E!10Q, E!11Q, E!12Q, and E!13Q.

Example # Configure a menu screencode of E!10Q.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc]menu screencode E!10Q
```

print connection-info

Syntax **print connection-info**

undo print connection-info

View Terminal template view

Parameters None

Description Use the **print connection-info** command to enable the printing of terminal connection information on the terminal.

Use the **undo print connection-info** command to disable the printing of terminal connection information.

By default, terminal connection information is printed on the terminal.

To facilitate your operation, after a TCP connection is established between the terminal and the FEP, the terminal will display a message indicating that the connection is successful. To disable the prompt message from being displayed, use the **undo print connection-info** command.

Make sure you enable the router to print characters on the terminal before using this command.

Related command: **print information**.

Example # Enable the printing of terminal connection information on the terminal

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] print connection-info
```

print information

Syntax **print information**

undo print information

View Terminal template view

Parameters None

Description Use the **print information** command to enable the router to print characters on the terminal.

Use the **undo print information** command to disable the router from printing characters on the terminal.

By default, the router can print characters on the terminal.

You can use this command when the terminal is connected to a printer for printing.

Related command: **print connection-info** and **print menu**.

Example # Disable the router from printing characters on the terminal.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] undo print information
```

print menu

Syntax **print menu**

undo print menu

View Terminal template view

Parameters None

Description Use the **print menu** command to print menu information on the terminal.

Use the **undo print menu** command to disable the printing of terminal menu information.

By default, terminal menu information is printed.

This command takes effect only in TTY and Telnet terminal access. Make sure you enable the router to print characters on the terminal before using this command.

Related command: **print information**.

Example # Enable the printing of terminal menu information on the terminal

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] print menu
```

print language

Syntax **print language** { **chinese** | **english** }

View Terminal template view

Parameters **chinese**: Prints prompt information in Chinese.

english: Prints prompt information in English.

Description Use the **print language** command to set the language of the printed prompt information.

By default, the prompt information is printed in Chinese on the terminal.

Example # Set the language of the prompt information printed on the terminal to English.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] print language english
```

redrawkey

Syntax **redrawkey** *ascii-code*&<1-3>

undo redrawkey

View Terminal template view

Parameters *ascii-code*&<1-3>: ASCII value of hotkey, ranging 1 to 255. "&<1-3>" means that you can provide up to three ASCII values.

Description Use the **redrawkey** command to set the hotkey for terminal redrawing.

Use the **undo redrawkey** command to cancel the hotkey configured for terminal redrawing.

By default, no hotkey is configured for terminal redrawing.

The terminal redrawing hotkey can be set in TTY terminal access only. Terminal redrawing works in a similar way as the screen saving function of VTY switching. When a terminal does not exhibit the normal terminal interface for some reasons (for example, when illegible characters appear), pressing the terminal redrawing hotkey can restore the original terminal interface.

- *Before performing terminal redrawing, you must add the screen 1 command to the configuration file ttyd on the FEP.*
- *The ASCII value of the redrawing hotkey configured must be different from that of any other hotkey configured on the device. Otherwise, hotkey conflicts will occur. For example, the hotkey value cannot be set to 17 or 19 because these two values are used for the hotkeys of flow control.*
- *Using the hotkey may not get a response rapidly when the terminal displays too much data.*

Example # Configure the terminal redrawing hotkey as <Ctrl+A> by setting its ASCII value to 1.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] redrawkey 1
```

reset rta connection

Syntax **reset rta connection** *terminal-number vty-number*

View User view

Parameters *terminal-number*: Terminal number, ranging 1 to 255.

vty-number: VTY number, ranging 0 to 7.

Description Use the **reset rta connection** command to forcibly tear down the TCP connection corresponding to a VTY of a terminal.

Example # Tear down the TCP connection corresponding to terminal 1.

```
<Sysname> reset rta connection 1 1
```

reset rta statistics

Syntax **reset rta statistics** *terminal-number*

View User view

Parameters *terminal-number*: Terminal number, ranging 1 to 255.

Description Use the **reset rta statistics** command to clear the statistics of a terminal.

Related command: **display rta**.

Example # Clear all the statistics about terminal 1.

```
<Sysname> reset rta statistics 1
```

resetkey

Syntax **resetkey** *ascii-code*&<1-3>

undo resetkey

View Terminal template view

Parameters *ascii-code*&<1-3>: ASCII value of a hotkey, ranging 1 to 255. "&<1-3>" means that you can provide up to three ASCII values.

Description Use the **resetkey** command to set the terminal reset hotkey.

Use the **undo resetkey** command to cancel the configured terminal reset hotkey.

By default, no terminal reset hotkey is configured.

After you press the terminal reset hotkey when a terminal fault occurs, the router tears down and then reestablishes the TCP connection with the FEP.

Note that the ASCII value of the redrawing hotkey configured must be different from that of any other hotkey configured on the device. Otherwise, hotkey conflicts will occur. For example, the hotkey value cannot be set to 17 or 19 because these two values are used for the hotkeys of flow control. Using the hotkey may not get a response rapidly when the terminal displays too much data.

Example # Configure the terminal reset hotkey as <Ctrl+A> by setting its ASCII value to 1.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] resetkey 1
```

rta bind

Syntax **rta bind** { **mac-address interface** *interface-type interface-number* | **string** *string* }

undo rta bind

View System view

Parameters **mac-address interface** *interface-type interface-number*: Uses the specified interface MAC address as the character string for router authentication. *interface-type interface-number*: Specifies a port by port type and port number.

string *string*: Uses a user-defined string for router authentication. *string* is a user-defined string of 1 to 30 characters.

Description Use the **rta bind** command to configure a character string for router authentication.

Use the **undo rta bind** command to restore the default.

By default, no authentication string is configured on the router.

This configuration is used to authenticate the connection between the router and the FEP. If the authentication succeeds (that is, the MAC address sent by the router and that configured on the FEP are consistent), the connection is established; otherwise, no connection can be established between the router and the FEP.

- *Only a MAC address or a character string can be configured at a time, and the latest configured one takes effect.*
- *The authentication type and character string configured on the router and FEP must be the same. Otherwise, the authentication fails and no connection can be established.*

Example # Bind the MAC address of Ethernet 0/0 for router authentication.

```
<Sysname> system-view
[Sysname] rta bind mac-address interface ethernet 0/0
```

Bind the character string abc for router authentication.

```
<Sysname> system-view
[Sysname] rta bind string abc
```

rta rtc-server listen-port

Syntax **rta rtc-server listen-port** *port-number*

undo rta rtc-server listen-port *port-number*

View System view

Parameters *port-number*: Listening TCP port number of the RTC server, ranging 1024 to 50000.

Description Use the **rta rtc-server listen-port** command to configure the listening port on the RTC server.

Use the **undo rta rtc-server listen-port** command to cancel the configured listening port.

By default, no listening port is configured on the RTC server.

Note that only one listening port can be configured.

Example # Configure the RTC server listening port number as 9010.

```
<Sysname> system-view
[Sysname] rta rtc-server listen-port 9010
```

rta server enable

Syntax **rta server enable**

undo rta server enable

View System view

Parameters None

Description Use the **rta server enable** command to enable terminal access on the router.

Use the **undo rta server enable** command to disable terminal access.

By default, terminal access is disabled on the router.

Note that, after terminal access is disabled, the settings of template, terminal, and VTY will be kept.

Example # Enable terminal access.

```
<Sysname> system-view
[Sysname] rta server enable
```

rta source-ip

Syntax **rta source-ip** *ip-address*

undo rta source-ip

View System view

Parameters *ip-address*: Source IP address used for establishing a TCP connection. It cannot be a loopback address, such as 127.0.0.1.

Description Use the **rta source-ip** command to configure the global source IP address of TCP connections.

Use the **undo rta source-ip** command to cancel the source IP address configured.

By default, no source IP address is configured globally for TCP connections.

- *You can use this command to configure an IP address other than the outbound interface's IP address of the initiating router as the TCP connection source IP address. Generally, the loopback interface or dialer interface of the router are used as the TCP connection source IP address for dial-up backup and address hiding.*
- *If a source IP address is also configured in a terminal template, this address is preferred as the source IP address for the corresponding terminal to establish TCP connections.*
- *After the global TCP connection source IP address is configured, a TCP connection must be reestablished for this address to take effect.*

Example # Set the global TCP connection source IP address to 1.1.1.1.

```
<Sysname> system-view
[Sysname] rta source-ip 1.1.1.1
```

rta template

Syntax **rta template** *template-name*

undo rta template *template-name*

View System view

Parameters *template-name*: Terminal template name, a string of 1 to 15 characters.

Description Use the **rta template** command to create a terminal template and enter terminal template view. If you specify an existing terminal template, you will enter the corresponding terminal template view.

Use the **undo rta template** command to delete a terminal template.

Example # Create terminal template abc and enter terminal template view.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc]
```

rta terminal

Syntax **rta terminal** *template-name terminal-number*

undo rta terminal

View Interface view

Parameters *template-name*: Terminal template name, a string of 1 to 15 characters.

terminal-number: Terminal number, ranging 1 to 255.

Description Use the **rta terminal** command to apply a template on the interface.

Use the **undo rta terminal** command to cancel the template application.

By default, no template is applied on the interface.

A terminal can be created only after the configured template is applied on the corresponding interface, so as to implement terminal access. Use the *terminal-number* argument to specify the terminal number. An interface can be connected to only one physical terminal. The router identifies physical terminals by terminal number.

Note that at least one VTY should be configured in the terminal template for the template to be applied on the interface. This command supports asynchronous serial interfaces, synchronous/asynchronous serial interfaces, and AUX interfaces. This command can be configured on a synchronous/asynchronous serial interface only when the interface operates in the asynchronous mode.

Example # Apply the terminal template abc with the terminal number of 1 on the interface.

```
<Sysname> system-view
[Sysname] interface async 1/1
[Sysname-rta-async1/1] rta terminal abc 1
```

sendbuf bufsize

Syntax **sendbuf bufsize** *size*

undo sendbuf bufsize

View Terminal template view

Parameters *size:* Maximum size of data sent to the terminal at one time, in bytes, ranging 2 to 500.

Description Use the **sendbuf bufsize** command to configure the maximum size of data to be sent to the terminal.

Use the **undo sendbuf bufsize** command to restore the default.

By default, the maximum size of data to be sent to the terminal at one time is 500 byes.

The router sends data in packets to the terminal. The sizes of the sent packets are different. Use the *size* argument to specify the maximum data packet size.

Example # Configure the maximum size of data to be sent at one time as 200 bytes.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] sendbuf bufsize 200
```

sendbuf threshold

Syntax **sendbuf threshold** *value*

undo sendbuf threshold

View Terminal template view

Parameters *value*: Threshold of terminal send buffer, in bytes, ranging 50 to 2,048.

Description Use the **sendbuf threshold** command to set the threshold of the terminal send buffer.

Use the **undo sendbuf threshold** command to cancel the configured threshold of the terminal send buffer.

By default, no threshold is configured.

The send buffer is used to store the data that the router is to send to the terminal. The threshold specifies the maximum data in bytes that the send buffer can store.

Example # Set the terminal send buffer threshold to 1,000 bytes.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] sendbuf threshold 1000
```

tcp

Syntax **tcp** { **keepalive** *time count* | **nodelay** | **recvbuf-size** *recvsize* | **sendbuf-size** *sendsize* }

undo tcp { **keepalive** | **nodelay** | **recvbuf-size** | **sendbuf-size** }

View Terminal template view

Parameters **keepalive** *time count*: Sets the parameters for sending TCP keepalives. *time* indicates the interval for sending keepalives, in seconds, ranging 10 to 7,200. *count* indicates the keepalive retransmission times, ranging 1 to 100.

nodelay: Specifies not to use the TCP Nagle algorithm, that is, no TCP delay.

recvbuf-size *recvsize*: TCP receive buffer size, in bytes, ranging 512 to 16,384.

sendbuf-size *sendsize*: TCP send buffer size, in bytes, ranging 512 to 16,384.

Description Use the **tcp** command to configure TCP parameters, including receive buffer size, send buffer size, no delay, keepalive interval, and number of keepalives to be sent.

Use the **undo tcp** command to restore the default TCP settings.

By default, receive buffer size is 2,048 bytes, send buffer size is 2,048 bytes, delay is enabled, keepalive interval is 50 seconds, and the number of keepalives is 3.

If you specify the **nodelay** keyword, the TCP Nagle algorithm will not be used.

Note that the newly configured TCP parameters take effect only after the connection is reestablished.

Example # Set the TCP receive buffer size to 512 bytes.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] tcp recvbuf-size 512
```

Set the TCP send buffer size to 512 bytes.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] tcp sendbuf-size 512
```

Disable TCP delay.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] tcp nodelay
```

Set the TCP keepalive interval to 1,800 seconds and the number of keepalives to 2.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] tcp keepalive 1800 2
```

testkey

Syntax **testkey** *ascii-code*&<1-3>

undo testkey

View Terminal template view

Parameters *ascii-code*&<1-3>: ASCII value of the hotkey, ranging 1 to 255. "&<1-3>" means that you can provide up to three ASCII values.

Description Use the **testkey** command to configure the terminal connectivity test hotkey.

Use the **undo testkey** command to cancel the hotkey configured.

By default, no hotkey is configured for connectivity test.

With the terminal connectivity test hotkey configured on the router, you can press the hotkey to test the TCP connectivity between the terminal and the router and that between the terminal and the FEP.

- *This command takes effect only in Telnet terminal access and TTY terminal access.*
- *The ASCII value of the hotkey configured must be different from that of any other hotkey configured on the device. Otherwise, hotkey conflicts will occur. For example, the hotkey value cannot be set to 17 or 19 because these two values are used for the hotkeys of flow control.*
- *Using the hotkey may not get a response rapidly when the terminal displays too much data.*

Example # Configure the terminal connectivity test hotkey as <Alt+A>, namely, 1 96 13.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] testkey 1 96 13
```

update changed-config

Syntax **update changed-config**

View Terminal template view

Parameters None

Description Use the **update changed-config** command to update template configurations.

If the template has been applied on the corresponding interface, the configurations made in template view will take effect after the **update changed-config** command is executed. You are recommended to complete all terminal template configurations before applying the template on the interface.

Note that some configurations, such as source IP address configuration and encryption, take effect only after they are updated and the connection is reestablished.

Example # Set the menu hotkey under the template and update the configuration for the hotkey to take effect.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] menu hotkey 1
[Sysname-rta-template-abc] update changed-config
```

vty description

Syntax **vty** *vty-number* **description** *string*

undo vty *vty-number* **description**

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

string: VTY description, a string of 1 to 31 characters.

Description Use the **vty description** command to configure a description for a VTY.

Use the **undo vty description** command to remove the description for a VTY.

By default, no description is configured for a VTY.

For a VTY of a service, you are recommended to use the service name as the description information of the VTY for convenience.

Example # Set the description information of VTY 1 to chuxu.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 description chuxu
```

vty hotkey

Syntax **vty** *vty-number* **hotkey** *ascii-code*&<1-3>

undo vty *vty-number* **hotkey**

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

ascii-code&<1-3>: ASCII value of the hotkey, ranging 1 to 255. "&<1-3>" means that you can provide up to three ASCII values.

Description Use the **vty** *vty-number* **hotkey** command to set the hotkey for VTY fast switching.

Use the **undo vty** *vty-number* **hotkey** command to cancel the hotkey configured.

By default, no hotkey is configured for VTY fast switching.

Terminal access supports VTY switching, allowing you to switch between applications. In terminal access, each terminal can be logically divided into eight

VTYs and each VTY corresponds to one application. When multiple VTYs are configured on a terminal with the corresponding switching hotkeys, you can press the switching hotkeys to quickly switch between the VTYs without making any selection on the menu. The connection of the original VTY application is not torn down. This way, dynamic switching between the VTYs (namely, different applications) on a terminal is implemented.

Note that the ASCII value of the hotkey configured must be different from that of any other hotkey configured on the device. Otherwise, hotkey conflicts will occur. For example, the hotkey value cannot be set to 17 or 19 because these two values are used for the hotkeys of flow control. Using a hotkey may not get a response rapidly when the terminal displays too much data.

Example # Configure the hotkey for VTY 1 as <Ctrl+A>, namely, 1.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 hotkey 1
```

vty password

Syntax **vty** *vty-number* **password** { **simple** | **cipher** } *string*

undo vty *vty-number* **password**

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

simple: Uses a plaint-text password that is displayed in plain text.

cipher: Uses a ciphertext password that is displayed in ciphertext.

string: Password. It is a plain-text string of 1 to 16 characters or a ciphertext string of 24 characters.

Description Use the **vty password** command to configure the password for VTY authentication.

Use the **undo vty password** command to cancel the password configured.

By default, no password is configured for VTY authentication.

Note that this command takes effect in RTC terminal access only and is used by the RTC server to authenticate RTC clients. To support terminal access authentication, passwords must be configured on the RTC server and the RTC clients, and authentication succeeds only if the passwords are the same. If authentication is not to be implemented, make sure no password is configured on the RTC server or any RTC client.

Example # Configure the authentication password for VTY 1 as abc.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 password simple abc
```

vty rtc-client remote

Syntax **vty** *vty-number* **rtc-client remote** *ip-address port-number* [**source** *source-ip*]

undo vty *vty-number*

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

ip-address: IP address of the RTC server.

port-number: Listening port number of the RTC server, ranging 1024 to 50000.

source *source-ip*: Source IP address bound.

Description Use the **vty rtc-client remote** command to create a VTY to serve as an RTC client.

Use the **undo vty** command to remove the specified VTY.

Note that, after this configuration, no more Telnet VTYs, TTY VTYs, or RTC server VTYs can be configured in the template of the VTY.

Related command: **rta rtc-server listen-port** and **vty rtc-server remote**.

Example # Create VTY 1 to serve as an RTC client, setting the IP address of the corresponding RTC server to 1.1.1.1, the listening port of the RTC server to 9010, and the source IP address to be used for establishing TCP connections to 2.2.2.2.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 rtc-client remote 1.1.1.1 9010 source 2.2.2.2
```

vty rtc-server remote

Syntax **vty** *vty-number* **rtc-server remote** *ip-address terminal-number*

undo vty *vty-number*

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

ip-address: RTC client IP address.

terminal-number: Terminal number corresponding to the RTC client, ranging 1 to 255.

Description Use the **vty rtc-server remote** command to create a VTY to serve as the RTC server.

Use the **undo vty** command to remove the specified VTY.

Note that, after this configuration, no more Telnet VTYs, TTY VTYs, or RTC client VTYs can be configured in the template of the VTY.

Example # Create a VTY to serve as the RTC server, setting the IP address of the RTC client to 2.2.2.2 and the terminal number to 1.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 rtc-server remote 2.2.2.2 1
```

vty screencode

Syntax **vty** *vty-number* **screencode** *string*

undo vty *vty-number* **screencode**

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

string: Terminal screen code, a string of 1 to 15 characters.

Description Use the **vty screencode** command to set the screen code for triggering screen saving.

Use the **undo vty screencode** command to cancel the screen code configured.

By default, no screen code is configured for terminal screen saving.

Some types of terminals provide the screen saving function. When such a terminal receives the specified screen code, such as E!10Q (for details about screen codes, refer to the related terminal manuals), it saves the current interface and switch to the corresponding screen.

Note that this function requires terminal support and the screen code configured on the router and that specified on the terminal must be the same. Screen codes configured vary with terminal types. For details, refer to the corresponding terminal manuals. For example, Start terminals support E!8Q, E!9Q, E!10Q, E!11Q, E!12Q, and E!13Q. To support screen saving and menu printing, the **menu screencode** command must be used.

Related command: **menu screencode**.

Example # Set the screen code for VTY 1 to E!9Q.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 screencode E!9Q
```

vty telnet remote

Syntax **vty** *vty-number* **telnet remote** *ip-address* [*port-number*] [**source** *source-ip*]

undo vty *vty-number*

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

ip-address: FEP IP address.

port-number: Listening Telnet port on the FEP. It ranges 1 to 50000 and defaults to 23.

source *source-ip*: Source IP address bound.

Description Use the **vty telnet remote** command to create a VTY for Telnet terminal access.

Use the **undo vty** command to remove the specified VTY.

Note that, after this configuration, no more RTC client VTYs or RTC server VTYs can be configured in the template of the VTY.

Example # Create a VTY for Telnet terminal access, setting the FEP IP address to 1.1.1.1.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 telnet remote 1.1.1.1
```

vty tty remote

Syntax **vty** *vty-number* **tty remote** *ip-address port-number* [**source** *source-ip*]

undo vty *vty-number*

View Terminal template view

Parameters *vty-number*: VTY number, ranging 0 to 7.

ip-address: FEP IP address.

port-number: Listening port number of the ttyd program on the FEP, ranging 1024 to 50000.

source *source-ip*: Source IP address bound.

Description Use the **vty tty remote** command to create a VTY for TTY terminal access.

Use the **undo vty** command to remove the specified VTY.

Note that, after this configuration, no more RTC client VTYs or RTC server VTYs can be configured in the template of the VTY.

Example # Create VTY 1 for TTY terminal access, setting FEP IP address to 1.1.1.1, listening port number to 9010, and source IP address to 2.2.2.2.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty 1 tty remote 1.1.1.1 9010 source 2.2.2.2
```

vty-switch priority

Syntax **vty-switch priority**

undo vty-switch priority

View Terminal template view

Parameters None

Description Use the **vty-switch priority** command to configure the RTC server to perform VTY switching based on priority.

Use the **undo vty-switch priority** command to restore the default setting.

By default, the VTY switching is performed not based on priority.

This command takes effect in RTC terminal access. When VTY switching is performed based on priority (the lower the VTY number, the higher the priority), if the VTY number corresponding to the connection request received is less than the VTY number corresponding to the existing connection, the RTC server tears down the existing connection and begins to use the new connection for communication. If a connection has been established and this command is not used, any newer connection will be torn down.

Example # Configure the RTC server to perform VTY switching based on priority.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty-switch priority
```

vty-switch threshold

Syntax **vty-switch threshold** *times*

undo vty-switch threshold

View Terminal template view

Parameters *times*: Threshold for VTY automatic switching, in times, ranging 1 to 1,0000.

Description Use the **vty-switch threshold** command to configure the threshold for VTY automatic switching.

Use the **undo vty-switch threshold** command to restore the default.

By default, no threshold is configured; that is, no switching is performed.

Note that this command takes effect only in RTC client terminal access. After this configuration, when an RTC client needs to initiate a connection to an RTC server, it first initiates a connection to the RTC server with the lowest VTY number. If the number of connection failures exceeds the threshold, the RTC client initiates a connection to the RTC server with the second lowest VTY number.

Example # Set the threshold for automatic VTY switching.

```
<Sysname> system-view
[Sysname] rta template abc
[Sysname-rta-template-abc] vty-switch threshold 5
```

71 IP ROUTING TABLE COMMANDS

bandwidth-based-sharing

Syntax **bandwidth-based-sharing**

undo bandwidth-based-sharing

View System view

Parameters None

Description Use the **bandwidth-based-sharing** command to enable bandwidth-based load sharing.

Use the **undo bandwidth-based-sharing** command to disable bandwidth-based load sharing.

By default, bandwidth-based load sharing is disabled.

If multiple outbound interfaces/nexthops to a destination are found during forwarding:

- When bandwidth-based load sharing is disabled, the packets are forwarded through all these interfaces in turn.
- When bandwidth-based load sharing is enabled, the device calculates the packet forwarding proportion for each interface based on the bandwidths and then determines through which interfaces to forward the subsequent packets (the number of packets already forwarded through these interfaces is considered).

Examples # Enable bandwidth-based load sharing.

```
<Sysname> system-view
[Sysname] bandwidth-based-sharing
```

display ip routing-table

Syntax **display ip routing-table** [**vpn-instance** *vpn-instance-name*] [**verbose**] | { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameters **vpn-instance** *vpn-instance-name*: Displays routing table information for a VPN instance. The *vpn-instance-name* argument represents the instance name and is a string of 1 to 31 characters.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only summary information about active routes.

|: Uses a regular expression to filter output information.

begin: Displays routing table entries starting from the one specified by the regular expression.

include: Displays routing table entries specified by the regular expression.

exclude: Displays routing table entries other than those specified by the regular expression.

regular-expression: Regular expression for filtering routing table entries, a string of 1 to 256 characters.

Table 201 Special characters for regular expressions

Character	Meaning	Remarks
_	Underscore, functions similarly as a wildcard and matches one of the following:	If it is not the first character in a regular expression, it can appear as many times as the command line length permits.
	(^|$|[,(){}])	If it is the first character in a regular expression, it can be followed with up to four underscores.
	or a space, the beginning of a string, the end of a string.	If it appears intermittently in a regular expression, only the first group takes effect.
(	Left parenthesis, represents a stack push operation in a program.	It is not recommended to use this character in a regular expression.
.	Full stop, a wildcard that matches any character, including a space.	-
*	Asterisk, indicates that the character(s) to its left can appear 0 or more times.	zo* matches z and zoo.
+	Plus, indicates that the character(s) to its left can appear one or more times.	zo+ matches zo and zoo, but not z.

Description Use the **display ip routing-table** command to display brief information about active routes in the routing table.

Use the **display ip routing-table verbose** command to display detailed information about all routes in the routing table.

Examples # Display brief information about active routes in the routing table.

```
<Sysname> display ip routing-table
Routing Tables: Public
         Destinations : 6        Routes : 6

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

2.2.2.0/24          Direct 0    0            2.2.2.1         Eth0/1
2.2.2.1/32          Direct 0    0            127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0            127.0.0.1       InLoop0
127.0.0.1/32        Direct 0    0            127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0            192.168.80.10   Eth0/1
192.168.80.10/32    Direct 0    0            127.0.0.1       InLoop0
```

Table 202 Description on the fields of the display ip routing-table command

Field	Description
Destinations	Number of destination addresses
Routes	Number of routes
Destination/Mask	Destination address/mask length
Proto	Protocol that presents the route
Pre	Priority of the route
Cost	Cost of the route
Nexthop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route

Display detailed information about all routes in the routing table.

```
<Sysname>display ip routing-table verbose
Routing Table : Public
         Destinations : 5        Routes : 5

  Destination: 10.1.1.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.1.1         Interface: Serial2/0
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h00m30s
          Tag: 0

  Destination: 10.1.1.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1        Interface: InLoopBack0
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active NoAdv           Age: 00h00m30s
          Tag: 0

  Destination: 10.1.1.2/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.1.2         Interface: Serial2/0
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h00m30s
          Tag: 0
```

```
Destination: 127.0.0.0/8
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 127.0.0.1        Interface: InLoopBack0
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active NoAdv           Age: 00h00m36s
        Tag: 0

Destination: 127.0.0.1/32
   Protocol: Direct          Process ID: 0
 Preference: 0                     Cost: 0
    NextHop: 127.0.0.1        Interface: InLoopBack0
RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
  Tunnel ID: 0x0                  Label: NULL
      State: Active NoAdv           Age: 00h00m36s
        Tag: 0
```

Displayed first are statistics for the whole routing table, followed by detailed description of each route (in sequence).

Table 203 Description on the fields of the display ip routing-table verbose command

Field	Description
Destination	Destination address/mask length
Protocol	Protocol that presents the route
Process ID	Process ID
Preference	Priority of the route
Cost	Cost of the route
NextHop	Address of the next hop on the route
Interface	Outbound interface for packets to be forwarded along the route
RelyNextHop	The next hop address obtained through routing stack.
Neighbour	Neighboring address determined by Routing Protocol
Tunnel ID	Tunnel ID
Label	Label
State	Status of the route, which could be Active, Inactive, Adv, or NoAdv.
Age	Time that the route has been in the routing table, in the sequence of hour, minute, and second from left to right.
Tag	Route tag

display ip routing-table acl

Syntax **display ip routing-table acl** *acl-number* [**verbose**]

View Any view

Parameters *acl-number*: Basic ACL number, in the range of 2000 to 2999.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description

Use the **display ip routing-table acl** command to display information about routes permitted by a specified basic ACL.

This command is intended for the follow-up display of routing policies.

For more information about routing policy, refer to "Routing Policy Common Configuration Commands" on page 1187.

If the specified ACL does not exist or it has no rules configured, the entire routing table is displayed.

Examples

Define basic ACL 2000 and set the route filtering rules.

```
<Sysname > system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule deny source any
```

Display brief information about active routes permitted by basic ACL 2000.

```
[Sysname-acl-basic-2000] display ip routing-table acl 2000
Routes Matched by Access list : 2000
Summary Count : 6

Destination/Mask    Proto  Pre  Cost         NextHop         Interface

10.1.1.0/24         Direct 0    0            10.1.1.2        Vlan1
10.1.1.2/32         Direct 0    0            127.0.0.1       InLoop0
10.1.2.0/24         Direct 0    0            10.1.2.1        Eth1/0
10.1.2.1/32         Direct 0    0            127.0.0.1       InLoop0
10.1.3.0/24         Direct 0    0            10.1.3.1        Eth1/1
10.1.3.1/32         Direct 0    0            127.0.0.1       InLoop0
```

For detailed description of the above output, see Table 202.

Display detailed information about both active and inactive routes permitted by basic ACL 2000.

```
<Sysname> display ip routing-table acl 2000 verbose
Routes Matched by Access list : 2000
Summary Count: 6

Destination: 10.1.1.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.1.2         Interface: Vlan1
  RelyNextHop: 0.0.0.0          Neighbour: 0.0.0.0
    Tunnel ID: 0x0                  Label: NULL
        State: Active Adv             Age: 00h25m32s
          Tag: 0

Destination: 10.1.1.2/32
```

```
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1       Interface: InLoop0
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                 Label: NULL
        State: Active NoAdv          Age: 00h41m34s
          Tag: 0
Destination: 10.1.2.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.2.1        Interface: Eth1/0
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                 Label: NULL
        State: Active Adv            Age: 00h05m42s
          Tag: 0

Destination: 10.1.2.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1       Interface: InLoop0
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                 Label: NULL
        State: Active NoAdv          Age: 00h05m42s
          Tag: 0
Destination: 10.1.3.0/24
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 10.1.3.1        Interface: Eth1/1
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                 Label: NULL
        State: Active Adv            Age: 00h05m31s
          Tag: 0

Destination: 10.1.3.1/32
     Protocol: Direct          Process ID: 0
   Preference: 0                     Cost: 0
      NextHop: 127.0.0.1       Interface: InLoop0
  RelyNextHop: 0.0.0.0         Neighbour: 0.0.0.0
    Tunnel ID: 0x0                 Label: NULL
        State: Active NoAdv          Age: 00h05m32s
          Tag: 0
```

Table 204 Description on the fields of the display ip routing-table command

Field	Description
Destination	Destination address
Mask	Mask
Protocol	Routing protocol that discovered the route
Preference	Preference of the route
Nexthop	Nexthop address
Interface	Outbound interface for packets to be forwarded along the route

Table 204 Description on the fields of the display ip routing-table command

Field	Description	
State	Route status:	
	ActiveU	This is an active unicast route. **U** means unicast.
	Blackhole	A blackhole route is similar with a reject route except that a router drops packets matching a blackhole route without sending ICMP unreachable messages to the source of the packets.
	Delete	This route is deleted.
	Gateway	This is an indirect route.
	Hidden	This route is hidden. For routes that are temporarily unusable for some reasons (because of a policy configured or because the interface is down), you can hide them for later use.
	Holddown	The route is suppressed. Holddown is a route advertisement policy used in some distance vector (D-V) routing protocols, such as RIP, to avoid the propagation of some incorrect routes and improve the transmission speed of unreachable route information. It distributes a certain route during a period regardless of whether a new route to the same destination is found. For details, refer to "IS-IS Configuration Commands" on page 1037 and "Multicast Routing and Forwarding Configuration Commands" on page 1327.
	Int	The route was discovered by an Internal Gateway Protocol (IGP).
	NoAdvise	The route is not advertised when the router advertises routes based on policies.
	NotInstall	Normally, the routes with the highest preference in the routing table are installed into the core routing table and are advertised, while the NotInstall routes cannot be installed into the core routing table but can be advertised.
	Reject	The packets matching a Reject route will be dropped. Besides, the router sends ICMP unreachable messages to the source of the dropped packets. The Reject routes are usually used for network testing.
	Retain	The Retain routes are not deleted when the routes read from the core routing table are deleted. You can keep static routes in the core routing table by configuring them as Retain routes.
	Static	A Static route are not lost when you perform the save operation and then restart the router. Routes configured manually are marked as **static**.
	Unicast	Unicast routes
Age	Age of the route in the routing table, in the form of hh:mm:ss.	
Cost	Route cost	

display ip routing-table ip-address

Syntax **display ip routing-table** *ip-address* [*mask-length* | *mask*] [**longer-match**] [**verbose**]

display ip routing-table *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } [**verbose**]

View Any view

Parameters *ip-address*: Destination IP address, in dotted decimal format.

mask-length: IP address mask length in the range 0 to 32.

mask: IP address mask in dotted decimal format.

longer-match: Displays the route with the longest prefix.

verbose: Displays detailed routing table information, including both active and inactive routes. With this keyword absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table** *ip-address* command to display information about routes to a specified destination address.

Executing the command with different parameters yields different output:

- **display ip routing-table** *ip-address*

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for an entry and this entry is active, it is displayed.

- **display ip routing-table** *ip-address mask*

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for an entry and the entry is active with a subnet mask less than or equal to the input subnet mask, the entry is displayed.

Only route entries that exactly match the input destination address and mask are displayed.

- **display ip routing-table** *ip-address* **longer-match**

The system ANDs the input destination IP address with the subnet mask in each route entry; and ANDs the destination IP address in each route entry with its corresponding subnet mask.

If the two operations yield the same result for multiple entries that are active, the one with longest mask length is displayed.

- **display ip routing-table** *ip-address mask* **longer-match**

The system ANDs the input destination IP address with the input subnet mask; and ANDs the destination IP address in each route entry with the input subnet mask.

If the two operations yield the same result for multiple entries with a mask less than or equal to the input subnet mask, the one that is active with longest mask length is displayed.

Use the **display ip routing-table** *ip-address1* { *mask-length* | *mask* } *ip-address2* { *mask-length* | *mask* } command to display route entries with destination addresses within a specified range.

Examples # Display route entries for the destination IP address 11.1.1.1.

```
[Sysname] display ip routing-table  11.1.1.1
Routing Table : Public
Summary Count : 4

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

0.0.0.0/0           Static 60   0            0.0.0.0         NULL0
11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

For detailed description about the output, see Table 204.

Display route entries by specifying a destination IP address and the **longer-match** keyword.

```
[Sysname] display ip routing-table  11.1.1.1 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask.

```
[Sysname] display ip routing-table  11.1.1.1 24
Routing Table : Public
Summary Count : 3

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

11.0.0.0/8          Static 60   0            0.0.0.0         NULL0
11.1.0.0/16         Static 60   0            0.0.0.0         NULL0
11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

Display route entries by specifying a destination IP address and mask and the **longer-match** keyword.

```
[Sysname] display ip routing-table  11.1.1.1 24 longer-match
Routing Table : Public
Summary Count : 1

Destination/Mask    Proto   Pre  Cost         NextHop         Interface

11.1.1.0/24         Static 60   0            0.0.0.0         NULL0
```

For detailed description of the above output, see Table 204.

Display route entries for destination addresses in the range 1.1.1.0 to 5.5.5.0.

```
<Sysname> display ip routing-table 1.1.1.0 24 5.5.5.0 24
Routing Table : Public

Destination/Mask    Proto   Pre  Cost         NextHop       Interface
```

```
1.1.1.0/24          Direct 0    0           1.1.1.1       Vlan1
1.1.1.1/32          Direct 0    0           127.0.0.1     InLoop0
2.2.2.0/24          Direct 0    0           2.2.2.1       Vlan2
3.3.3.0/24          Direct 0    0           3.3.3.1       Eth1/0
3.3.3.1/32          Direct 0    0           127.0.0.1     InLoop0
4.4.4.0/24          Direct 0    0           4.4.4.1       Eth1/1
4.4.4.1/32          Direct 0    0           127.0.0.1     InLoop0
```

display ip routing-table ip-prefix

Syntax **display ip routing-table ip-prefix** *ip-prefix-name* [**verbose**]

View Any view

Parameters *ip-prefix-name*: IP Prefix list name, a string of 1 to 19 characters.

verbose: Displays detailed routing table information, including that for inactive routes. With this argument absent, the command displays only brief information about active routes.

Description Use the **display ip routing-table ip-prefix** command to display information about routes permitted by a specified prefix list.

This command is intended for the follow-up display of routing policies. If the specified prefix list is not configured, detailed information about all routes (with the **verbose** keyword) or brief information about all active routes (without the **verbose** keyword) is displayed.

Examples # Configure a prefix list named **test**, permitting routes with a prefix of 2.2.2.0 and a mask length between 24 and 32.

```
<Sysname> system-view
[Sysname] ip ip-prefix test permit 2.2.2.0 24 less-equal 32
```

Display brief information about active routes permitted by the prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test
Routes Matched by Prefix list : test
Summary Count : 2
Destination/Mask   Proto  Pre  Cost        NextHop         Interface
2.2.2.0/24         Direct  0    0          2.2.2.1         Vlan2
2.2.2.1/32         Direct  0    0          127.0.0.1       InLoop0
```

For detailed description of the above output, see Table 204.

Display detailed information about both active and inactive routes permitted by IP prefix list **test**.

```
[Sysname] display ip routing-table ip-prefix test verbose
Routes Matched by Prefix list  test :
Summary Count : 2

Destination: 2.2.2.0/24
```

```
     Protocol: Direct                  Process ID: 0
   Preference: 0                             Cost: 0
      NextHop: 2.2.2.1                Interface: Vlan2
  RelyNextHop: 0.0.0.0                Neighbour: 0.0.0.0
    Tunnel ID: 0x0                        Label: NULL
        State: Active Adv                   Age: 00h20m52s
          Tag: 0

Destination: 2.2.2.1/32
     Protocol: Direct                  Process ID: 0
   Preference: 0                             Cost: 0
      NextHop: 127.0.0.1              Interface: InLoop0
  RelyNextHop: 0.0.0.0                Neighbour: 0.0.0.0
    Tunnel ID: 0x0                        Label: NULL
        State: Active NoAdv                 Age: 00h20m52s
          Tag: 0
```

For detailed description of the above output, see Table 204.

display ip routing-table protocol

Syntax **display ip routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Displays the routes of a routing protocol, not including routes redistributed into the protocol. It can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

inactive: Displays only inactive routes. With this argument absent, the command displays information about both active and inactive routes.

verbose: Displays detailed routing information. With this argument absent, the command displays brief routing information.

Description Use the **display ip routing-table protocol** command to display routing information of a specified routing protocol.

Examples # Display brief information about direct routes.

```
<Sysname> display ip routing-table protocol direct
Public Routing Table : Direct
Summary Count : 6

Direct Routing table Status : < Active>
Summary Count :  6

Destination/Mask    Proto  Pre  Cost       NextHop         Interface

2.2.2.0/24          Direct 0    0          2.2.2.1         Vlan2
2.2.2.2/32          Direct 0    0          127.0.0.1       InLoop0
127.0.0.0/8         Direct 0    0          127.0.0.1       InLoop0
127.0.0.1/32          Direct 0    0          127.0.0.1       InLoop0
192.168.80.0/24     Direct 0    0          192.168.80.10   Eth1/0
192.168.80.10/32    Direct 0    0          127.0.0.1       InLoop0
```

```
Direct Routing table Status : < Inactive>
Summary Count : 0
```

Display summary information about static routes.

```
<Sysname> display ip routing-table protocol static
Public Routing Table : Static
Summary Count : 2

Static Routing table Status : < Active>
Summary Count :  0

Static Routing table Status : < Inactive>
Summary Count : 2
Destination/Mask    Proto   Pre  Cost       NextHop      Interface
1.2.3.0/24          Static  60   0          1.2.4.5      Vlan10
3.0.0.0/8           Static  60   0           2.2.2.2     Eth1/0
```

For detailed description of the above output, see Table 204.

display ip routing-table statistics

Syntax **display ip routing-table** [**vpn-instance** *vpn-instance-name*] **statistics**

View Any view

Parameters **vpn-instance** *vpn-instance-name*: Displays routing table information for a VPN instance. The VPN instance name is a string of 1 to 31 characters.

Description Use the **display ip routing-table statistics** command to display statistics about the public network routing table or a VPN routing table.

Examples # Display statistics about the routes in the routing table.

```
<Sysname> display ip routing-table statistics
Proto      route       active      added       deleted       freed
DIRECT     24          4           25          1             0
STATIC     4           1           4           0             0
RIP        0           0           0           0             0
OSPF       0           0           0           0             0
IS-IS      0           0           0           0             0
BGP        0           0           0           0             0
Total      28          5           29          1             0
```

Table 205 Description on the fields of the display ip routing-table statistics command

Field	Description
Proto	Origin of the routes. Possible values include O_ASE for OSPF_ASE routes, O_NSSA for OSPF NSSA, and AGGRE for aggregated routes.
route	Number of routes from the origin
active	Number of active routes from the origin
added	Number of routes added into the routing table since the router starts up or the last routing table reset operation

Table 205 Description on the fields of the display ip routing-table statistics command

Field	Description
deleted	Number of routes marked as deleted, which will be freed after a period.
freed	Number of routes that got freed, that is, got removed permanently
Total	Sums for the numerical items above

display ip relay-route

Syntax **display ip relay-route** [**vpn-instance** *vpn-instance-name*]

View Any view

Parameters **vpn-instance** *vpn-instance-name*: Displays the recursive route information of the VPN instance. *vpn-instance-name* is a string of 1 to 31 characters.

Description Use the **display ip relay-route** command to display the information of recursive routes.

When executed with no argument, this command displays the recursive route information of the public network routing table.

Examples # Display recursive route information.

```
<Sysname> display ip relay-route
 Total Number of Relay-route is: 1.
 Dest/Mask: 40.40.40.0/255.255.255.0
        Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 206 Description on the fields of the display ip relay-route command

Field	Description
Total Number of Relay-route	Total number of recursive routes
Dest/Mask	Destination address/mask of the recursive route
Related instance id(s)	The number in the parentheses after each instance ID indicates the number of routes that have used the recursive route in the routing table corresponding to the instance ID.

display ip relay-tunnel

Syntax **display ip relay-tunnel**

View Any view

Parameters None

Description Use the **display ip relay-tunnel** command to display recursive tunnel information.

Examples # Display recursive tunnel information.

```
<Sysname> display ip relay-tunnel
 Total Number of Relay-tunnel is: 1.
 Dest/Mask: 40.40.40.40/255.255.255.255
       Related instance id(s): 1(1) 2(1) 3(1) 4(1)
```

Table 207 Description on the fields of the display ip relay-tunnel command

Field	Description
Total Number of Relay-tunnel	Total number of recursive tunnels
Dest/Mask	Destination address/mask of the recursive tunnel
Related instance id(s)	The number in the parentheses after each instance ID indicates the number of routes that have used the recursive tunnel in the routing table corresponding to the instance ID.

display load-sharing ip address

Syntax **display load-sharing ip address** *ip-address { mask | mask-length }*

View Any view

Parameters *ip-address*: Destination IP address, in dotted decimal notation.

mask: IP address mask, in dotted decimal notation.

mask-length:IP address mask length, in the range 0 to 32.

Description Use the **display load-sharing ip address** command to display statistics about interface bandwidth-based non-balanced load sharing.

Examples # Display the statistics about bandwidth-based load sharing.

```
<Sysname> display load-sharing ip address 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop     Packet(s)   Bandwidth[KB]   Flow(s)     Interface
10.1.1.2        763851      100000          0           Ethernet0/0/0
10.1.2.2        1193501     155000          0           Atm1/0/0
10.1.3.2        15914       2048                0           Serial2/0/0
```

Table 208 Description on the fields of the display load-sharing ip address command

Field	Description
Nexthop	Nexthop address
Packet	Total number of packets forwarded through the outbound interface
Bandwidth	Bandwidth of the outbound interface used for load sharing
Flow	Number of flows fast forwarded through the outbound interface
Interface	Name of the outbound interface

display ipv6 routing-table

Syntax **display ipv6 routing-table**

View Any view

Parameters None

Description Use the **display ipv6 routing-table** command to display brief routing table information, including destination IP address and prefix, protocol type, priority, metric, next hop and outbound interface.

The command displays only active routes, namely, the brief information about the current optimal routes.

Examples # Display brief routing table information

```
<Sysname> display ipv6 routing-table
Routing Table :
        Destinations : 1        Routes : 1

Destination : ::1/128                           Protocol    : Direct
NextHop     : ::1                               Preference  : 0
Interface   : InLoop0                           Cost        : 0
```

Table 209 Description on the fields of the display ipv6 routing-table command

Field	Description
Destination	Destination IPv6 address
NextHop	Next hop
Preference	Routing preference
Interface	Outbound interface
Protocol	Routing protocol of the route
Cost	Routing cost

display ipv6 routing-table acl

Syntax **display ipv6 routing-table acl** *acl6-number* [**verbose**]

View Any view

Parameters *acl6-number:* Basic IPv6 ACL number, in the range 2000 to 2999.

Verbose: Displays both active and inactive verbose routing information permitted by the ACL. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table acl** command to display routing information permitted by the IPv6 ACL.

If the specified IPv6 ACL is not available, all routing information is displayed.

Examples # Display brief routing information permitted by ACL 2000.

```
<Sysname> display ipv6 routing-table acl 2000
Routes Matched by Access list  2000  :
```

```
Summary Count : 2

Destination : ::1/128                          Protocol   : Direct
NextHop     : ::1                              Preference : 0
Interface   : InLoop0                          Cost       : 0
Destination : 1:1::/64                           Protocol   : Static
NextHop     : ::                               Preference : 60
Interface   : NULL0                            Cost       : 0
```

Refer to Table 209 for description about the above output.

display ipv6 routing-table ipv6-address

Syntax **display ipv6 routing-table** *ipv6-address prefix-length* [**longer-match**] [**verbose**]

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length, in the range 0 to 128.

longer-match: Displays the matched route having the longest prefix length.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address* command to display routing information about the specified destination IPv6 address.

Executing the command with different parameters yields different output:

- **display ipv6 routing-table** *ipv6-address prefix-length*

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for an entry and the entry is active with a prefix length less than or equal to the input prefix length, the entry is displayed.

Only route entries that exactly match the input destination address and prefix length are displayed.

- **display ipv6 routing-table** *ipv6-address prefix-length* **longer-match**

The system ANDs the input destination IPv6 address with the input prefix length, and ANDs the destination IPv6 address in each route entry with the input prefix length.

If the two operations yield the same result for multiple entries with a prefix length less than or equal to the input prefix length, the one that is active with the longest prefix length is displayed.

Examples # Display brief routing information for the specified destination IPv6 address and prefix.

```
<Sysname> display ipv6 routing-table 10::1 127
Routing Table:
Summary Count: 3
Destination: 10::/64                                    Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
Destination: 10::/68                                    Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
Destination: 10::/120                                    Protocol  : Static
NextHop    : ::                                          Preference: 60
Interface  : NULL0                                       Cost      : 0
```

Display brief information about the matched route with the longest prefix length.

```
<Sysname> display ipv6 routing-table 10:: 127 longer-match
Routing Tables:
Summary Count : 1
Destination: 10::/120                                    Protocol  : Static
NextHop    : ::                                          Preference: 60
Interface  : NULL0                                       Cost      : 0
```

Refer to Table 209 for description about the above output.

display ipv6 routing-table ipv6-address1 ipv6-address2

Syntax **display ipv6 routing-table** *ipv6-address1 prefix-length1 ipv6-address2 prefix-length2* [**verbose**]

View Any view

Parameters *ipv6-address1*/*ipv6-address2*: An IPv6 address range from IPv6 address1 to IPv6 address2.

prefix-length1/*prefix-length2*: Prefix length, in the range 0 to 128.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table** *ipv6-address1 ipv6-address2* command to display routes with destinations falling into the specified IPv6 address range.

Examples # Display routes with destinations falling into the IPv6 address range.

```
<Sysname> display ipv6 routing-table 3:: 32 4:4:: 64
Routing Table :
Summary Count : 3

Destination: 100::/64                                    Protocol  : Static
NextHop    : ::                                          Preference: 60
Interface  : NULL0                                       Cost      : 0

Destination: 200::/64                                    Protocol  : Static
NextHop    : ::                                          Preference: 60
```

```
Interface  : NULL0                                      Cost      : 0

Destination: 300::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Refer to Table 209 for description about the above output.

display ipv6 routing-table ipv6-prefix

Syntax **display ipv6 routing-table ipv6-prefix** *ipv6-prefix-name* [**verbose**]

View Any view

Parameters *ipv6-prefix-name*: Name of the IPv6 prefix list, in the range 1 to 19 characters.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table ipv6-prefix** command to display routes permitted by the IPv6 prefix list.

Examples # Display brief active routing information permitted by the IPv6 prefix list **abc2**.

```
<Sysname> display ipv6 routing-table ipv6-prefix abc2
Routes Matched by Prefix list  abc  :
Summary Count : 1
Destination: 100::/64                                   Protocol  : Static
NextHop    : ::                                         Preference: 60
Interface  : NULL0                                      Cost      : 0
```

Refer to Table 209 for description about the above output.

display ipv6 routing-table protocol

Syntax **display ipv6 routing-table protocol** *protocol* [**inactive** | **verbose**]

View Any view

Parameters *protocol*: Displays the routes of a routing protocol, not including routes redistributed into the protocol. The protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** or **static**.

inactive: Displays only inactive routes. Without the keyword, all active and inactive routes are displayed.

verbose: Displays both active and inactive verbose routing information. Without this keyword, only brief active routing information is displayed.

Description Use the **display ipv6 routing-table protocol** command to display routes of a specified routing protocol.

Examples # Display brief information about all direct routes.

```
<Sysname> display ipv6 routing-table protocol direct
Direct Routing Table :
Summary Count : 1

Direct Routing Table's Status : < Active >
Summary Count : 1

Destination: ::1/128                                    Protocol  : Direct
NextHop    : ::1                                        Preference: 0
Interface  : InLoop0                                    Cost      : 0

Direct Routing Table's Status : < Inactive >
Summary Count : 0
```

Refer to Table 209 for description about the above output.

display ipv6 routing-table statistics

Syntax **display ipv6 routing-table statistics**

View Any view

Parameters None

Description Use the **display ipv6 routing-table statistics** command to display routing statistics, including total route number, added route number and deleted route number.

Examples # Display routing statistics.

```
<Sysname> display ipv6 routing-table statistics
Protocol   route      active     added      deleted     freed
DIRECT      1           1          1           0           0
STATIC      3           0          3           0           0
RIPng       0           0          0           0           0
OSPFv3      0           0          0           0           0
IS-ISv6     0           0          0           0           0
BGP4+       0           0          0           0           0
Total       4           1          4           0           0
```

Table 210 Description on the fields of the display ipv6 routing-table statistics command

Field	Description
Protocol	Routing protocol
route	Route number of the protocol
active	Active route number
added	Routes added after the last startup of the router
deleted	Deleted routes, which will be released after a specified time
freed	Released (totally removed from the routing table) route number
Total	Total route number

display ipv6 routing-table verbose

Syntax **display ipv6 routing-table verbose**

View Any view

Parameters None

Description Use the **display ipv6 routing-table verbose** command to display detailed information about all active and inactive routes, including the statistics of the entire routing table and information for each route.

Examples # Display detailed information about all active and inactive routes.

```
<Sysname> display ipv6 routing-table verbose
Routing Table :
         Destinations : 1        Routes : 1

 Destination  : ::1                                    PrefixLength : 128
 NextHop      : ::1                                    Preference   : 0
 RelayNextHop : ::                                     Tag          : 0H
 Neighbour    : ::                                     ProcessID    : 0
 Interface    : InLoopBack0                            Protocol     : Direct
 State        : Active NoAdv                           Cost         : 0
 Tunnel ID    : 0x0                                    Label        : NULL
 Age          : 22161sec
```

Table 211 Description on the fields of the display ipv6 routing-table verbose command

Field	Description
Destination	Destination IPv6 address
PrefixLength	Prefix length of the address
Nexthop	Next hop
Preference	Routing preference
RelayNextHop	Relay next hop
Tag	Tag of the route
Neighbour	Neighbor address
ProcessID	Process ID
Interface	Outbound interface
Protocol	Routing protocol
State	State of the route, Active, Inactive, Adv (advertised), or NoAdv (not advertised)
Cost	Cost of the route
Tunnel ID	Tunnel ID
Label	Label
Age	Time that has elapsed since the route was generated

display ipv6 relay-route

Syntax **display ipv6 relay-route**

View Any view

Parameters None

Description Use the **display ipv6 relay-route** command to display IPv6 recursive route information.

Examples # Display IPv6 recursive route information.

```
<Sysname> display ipv6 relay-route
 Total Number of relay-route is: 1
 Dest/Mask: 192::1/64
      Related instance id(always 0): 0(1)
```

Table 212 Description on the fields of the display ipv6 relay-route command

Field	Description
Total Number of Relay-route	Total number of recursive routes
Dest/Mask	Destination address/mask of the recursive route
Related instance id(always 0)	IPv6 supports public networks only. Therefore, the instance ID can be 0 only. The number in the parentheses after the instance ID indicates the number of routes that have used the recursive route in the routing table.

display ipv6 relay-tunnel

Syntax **display ipv6 relay-tunnel**

View Any view

Parameters None

Description Use the **display ipv6 relay-tunnel** command to display IPv6 recursive tunnel information.

Examples # Display IPv6 recursive tunnel information.

```
<Sysname> display ipv6 relay-tunnel
 Total Number of relay-tunnel is: 1.
 Dest/Mask: 192::0/64
      Related instance id(always 0): 0(1)
```

Table 213 Description on the fields of the display ipv6 relay-tunnel command

Field	Description
Total Number of Relay-tunnel	Total number of recursive tunnels
Dest/Mask	Destination address/mask of the recursive tunnel
Related instance id(always 0)	IPv6 supports public networks only. Therefore, the instance ID can be 0 only. The number in the parentheses after the instance ID indicates the number of routes that have used the recursive tunnel in the routing table.

load-bandwidth

Syntax **load-bandwidth** *bandwidth*

undo load-bandwidth

View Interface view

Parameters *bandwidth*: Specifies the load sharing bandwidth for the interface.

Description Use the **load-bandwidth** *bandwidth* command to specify the load sharing bandwidth of the interface.

Use the **undo load-bandwidth** command to restore the default.

The load sharing bandwidth of an interface defaults to the physical bandwidth of the interface.

Examples # Configure the load sharing bandwidth of the interface.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] load-bandwidth 100
```

reset load-sharing

Syntax **reset load-sharing statistics ip address** *ip-address { mask | mask-length }*

reset load-sharing statistics all

View User view

Parameters *ip-address*: Destination IP address, in dotted decimal notation.

mask: IP address mask, in dotted decimal notation.

mask-length:IP address mask length, in the range 0 to 32.

Description Use the **reset load-sharing ip address** command to clear the statistics of non-balanced load sharing. This command clears the load sharing statistics of all the outbound interfaces corresponding to the destination IP address.

Use the **reset load-sharing all** command to clear the load sharing statistics of the outbound interfaces of all the forwarding entries.

Examples # Display the statistics of bandwidth-based load sharing.

```
<Sysname> display load-sharing ip address 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop     Packet(s)   Bandwidth[KB]   Flow(s)     Interface
10.1.1.2        763851      100000          0           Ethernet0/0/0
```

```
10.1.2.2        1193501     155000          0           Atm1/0/0
10.1.3.2        15914       2048                0           Serial2/0/0
```

Clear the statistics of bandwidth-based load sharing.

```
<Sysname> reset load-sharing statistics ip address 10.2.1.0 24
There are/is totally 3 route entry(s) to the same destination network.
Nexthop     Packet(s)   Bandwidth[KB]   Flow(s)     Interface
10.1.1.2        0           100000          0           Ethernet0/0/0
10.1.2.2        0           155000          0           Atm1/0/0
10.1.3.2        0           2048                0           Serial2/0/0
```

reset ip routing-table statistics protocol

Syntax **reset ip routing-table statistics protocol** [**vpn-instance** *vpn-instance-name*] { **all** | *protocol* }

View User view

Parameters *vpn-instance-name*: VPN instance name, a string of 1 to 31 characters.

all: Clears the routing statistics of all the routing protocols in the IPv4 routing table.

protocol: Clears the routing statistics of the specified routing protocol in the IPv6 routing table. At present, this argument can be **bgp**, **direct**, **is-is**, **ospf**, **rip**, or **static**.

Description Use the **reset ip routing-table statistics protocol** command to clear routing statistics for the routing table or VPN routing table.

Examples # Clear the routing statistics for the VPN instance **Sysname1**.

```
<Sysname> reset ip routing-table statistics protocol vpn-instance Sy
sname1 all
```

reset ipv6 routing-table statistics

Syntax **reset ipv6 routing-table statistics protocol** { **all** | *protocol* }

View User view

Parameters **all**: Clears the routing statistics of all the routing protocols in the IPv6 routing table.

protocol: Clears the routing statistics of the specified routing protocol in the IPv6 routing table. At present, this argument can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

Description Use the **reset ipv6 routing-table statistics** command to clear IPv6 routing table statistics.

Examples # Clear the routing statistics of all the routing protocols in the routing table.

```
<Sysname> reset ipv6 routing-table statistics protocol all
```

72 BGP CONFIGURATION COMMANDS

For routing policy configuration commands, refer to "Routing Policy Common Configuration Commands" on page 1187.

aggregate

Syntax **aggregate** *ip-address* { *mask* | *mask-length* } [**as-set** | **attribute-policy** *route-policy-name* | **detail-suppressed** | **origin-policy** *route-policy-name* | **suppress-policy** *route-policy-name*] *

undo aggregate *ip-address* { *mask* | *mask-length* }

View BGP view/BGP-VPN instance view

Parameters *ip-address*: Destination IP address of summary route.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range 0 to 32.

as-set: Creates a summary with AS set.

attribute-policy *route-policy-name:* Sets the attributes of the summary route according to the routing policy, the name of which is a string of 1 to 19 characters.

detail-suppressed: Only advertises the summary route.

suppress-policy *route-policy-name*: Suppresses specific routes defined in the routing policy, the name of which is a string of 1 to 19 characters.

origin-policy *route-policy-name*: References the routing policy to specify routes for summarization. The policy name is a string of 1 to 19 characters.

The keywords of the command are described as follows:

Table 214 Functions of the keywords

Keywords	Function
as-set	Used to create a summary route, whose AS path contains the AS path information of summarized routes. Use this keyword carefully when many AS paths need to be summarized, because the frequent changes of routes may lead to route oscillation.

Table 214 Functions of the keywords

Keywords	Function
detail-suppressed	This keyword does not suppress the summary route, but it suppresses the advertisement of all the more specific routes. To summarize only some specific routes, use the **peer filter-policy** command.
suppress-policy	Used to create a summary route and suppress the advertisement of some summarized routes. If you want to suppress some routes selectively and leave other routes still advertised, use the **if-match** clause of the **route-policy** command.
origin-policy	Selects only routes satisfying the routing policy for route summarization
attribute-policy	Sets attributes except the AS-PATH attribute for the summary route. The same work can be done by using the **peer route-policy** command.

Description Use the **aggregate** command to create a summary route in the BGP routing table.

Use the **undo aggregate** command to remove a summary route.

By default, no summary route is configured.

Examples # In BGP view, create a summary of 192.213.0.0/16 in the BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] aggregate 192.213.0.0 255.255.0.0
```

In BGP-VPN instance view, create a summary of 192.213.0.0/16 in BGP routing table (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] aggregate 192.213.0.0 255.255.0.0
```

balance (BGP/BGP-VPN instance view)

Syntax **balance** *number*

undo balance

View BGP view/VPN instance view

Parameters *number*: Number of BGP routes for load balancing, in the range 1 to 8. When it is set to 1, no load balancing is available.

Description Use the **balance** command to configure the number of BGP routes for load balancing.

Use the **undo balance** command to disable load balancing.

By default, no load balancing is configured.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing using route selection rules.

Related commands: **display bgp routing-table**.

Examples # In BGP view, set the number of routes participating in BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] balance 2
```

In BGP-VPN instance view, set the number of routes participating in BGP load balancing to 2 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] balance 2
```

bestroute as-path-neglect (BGP/BGP-VPN instance view)

Syntax **bestroute as-path-neglect**

undo bestroute as-path-neglect

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute as-path-neglect** command to configure the BGP router to not evaluate the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the BGP router to take the AS_PATH as a factor during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples # In BGP view, ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute as-path-neglect
```

In BGP-VPN instance view, ignore AS_PATH in route selection (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute as-path-neglect
```

bestroute compare-med (BGP/BGP-VPN instance view)

Syntax **bestroute compare-med**

undo bestroute compare-med

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

Examples # In BGP view, enable the comparison of MEDs for paths from each AS when selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute compare-med
```

In BGP-VPN instance view, enable the comparison of MED for paths from each AS when selecting the best route. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute compare-med
```

bestroute med-confederation (BGP/BGP-VPN instance view)

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers to select the optimal route.

Use the **undo bestroute med-confederation** command to disable the comparison.

The comparison is not enabled by default.

The system only compares MED values for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples # In BGP view, enable the comparison of the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] bestroute med-confederation
```

In BGP-VPN instance view, enable the comparison of the MED for paths from peers within the confederation. (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] bestroute med-confederation
```

bgp

Syntax **bgp** *as-number*

undo bgp [*as-number*]

View System view

Parameters *as-number*: Specifies the local AS number from 1 to 65535.

Description Use the **bgp** command to enable BGP and enter the BGP view.

Use the **undo bgp** command to disable BGP.

By default, BGP is not enabled.

Examples # Enable BGP and set local AS number to 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp]
```

compare-different-as-med (BGP/BGP-VPN instance view)

Syntax **compare-different-as-med**

undo compare-different-as-med

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths for one destination available, the path with the smallest MED is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples # In BGP view, enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] compare-different-as-med
```

In BGP-VPN instance view, enable to compare the MED for paths from peers in different ASs (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] compare-different-as-med
```

confederation id

Syntax **confederation id** *as-number*

undo confederation id

View BGP view

Parameters *as-number*: Number of the AS that contains multiple sub-ASs, in the range 1 to 65535.

Description Use the **confederation id** command to configure a confederation ID.

Use the **undo confederation id** command to remove a specified confederation.

By default, no confederation ID is configured.

Configuring a confederation can reduce IBGP connections in a large AS. You can split the AS into several sub-ASs, and each sub-AS remains fully meshed. These sub-ASs form a confederation. Key IGP attributes of a route, such as the next hop, MED, local preference, are not discarded when crossing each sub-AS. The sub-ASs still look like a whole from the perspective of other ASs. This can ensure the integrity of the former AS, and solve the problem of too many IBGP connections in the AS.

Related commands: **confederation nonstandard** and **confederation peer-as**.

Examples # Confederation 9 consists of four sub-ASs, namely, 38, 39, 40 and 41. The peer 10.1.1.1 is a member of the confederation while the peer 200.1.1.1 is outside of the confederation. Take sub AS 41 as an example.

```
<Sysname> system-view
[Sysname] bgp 41
[Sysname-bgp] confederation id 9
[Sysname-bgp] confederation peer-as 38 39 40
[Sysname-bgp] group Confed38 external
[Sysname-bgp] peer Confed38 as-number 38
[Sysname-bgp] peer 10.1.1.1 group Confed38
[Sysname-bgp] group Remote98 external
[Sysname-bgp] peer Remote98 as-number 98
[Sysname-bgp] peer 200.1.1.1 group Remote98
```

confederation nonstandard

Syntax **confederation nonstandard**

undo confederation nonstandard

View BGP view

Parameters None

Description Use the **confederation nonstandard** command to make the router compatible with routers not compliant with RFC3065 in the confederation.

Use the **undo confederation nonstandard** command to restore the default.

By default, all routers in the confederation comply with RFC3065.

All devices in the confederation should be configured with this command to interact with those devices not compliant with RFC3065.

Related commands: **confederation id** and **confederation peer-as**.

Examples # AS100 contains routers not compliant with RFC3065 and comprises two sub-ASs, 64000 and 65000.

```
<Sysname> system-view
[Sysname] bgp 64000
[Sysname-bgp] confederation id 100
[Sysname-bgp] confederation peer-as 65000
[Sysname-bgp] confederation nonstandard
```

confederation peer-as

Syntax **confederation peer-as** *as-number-list*

undo confederation peer-as [*as-number-list*]

View BGP view

Parameters *as-number-list*: Sub-AS number list. Up to 32 sub-ASs can be configured in one command line. The expression is *as-number-list* = a*s-number* &<1-32>, in which a*s-number* specifies a sub-AS number, and &<1-32> indicates up to 32 numbers can be specified.

Description Use the **confederation peer-as** command to specify confederation peer sub-ASs.

Use the **undo confederation peer-as** command to remove specified confederation peer sub-ASs.

By default, no confederation peer sub-ASs are configured.

Before this configuration, the **confederation id** command must be used to specify the confederation for the sub-ASs.

If the **undo confederation peer-as** command without the *as-number-list* argument is used, all confederation peer sub-ASs are removed.

Related commands: **confederation nonstandard** and **confederation id**.

Examples # Specify confederation peer sub ASs 2000 and 2001.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] confederation id 10
[Sysname-bgp] confederation peer-as 2000 2001
```

dampening (BGP/BGP-VPN instance view)

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View BGP view/BGP-VPN instance view

Parameters *half-life-reachable*: Specifies a half-life for active routes from 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies a half-life for suppressed routes from 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies a reuse threshold value for suppressed routes from 1 to 20000. A suppressed route whose penalty value decreases under the value is reused. By default, the reuse value is 750.

suppress: Specifies a suppression threshold from 1 to 20000. The route with a penalty value higher than the threshold is suppressed. The default value is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

*half-life-reachable, half-life-unreachable, reuse, suppres*s and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable BGP route dampening and/or configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

The command dampens only EBGP routes rather than IBGP routes.

Related commands: **reset bgp dampening**, **reset bgp flap-info**, **display bgp routing-table dampened**, **display bgp routing-table dampening parameter** and **display bgp routing-table flap-info**.

Examples # In BGP view, configure BGP route dampening.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] dampening 15 15 1000 2000 10000
```

In BGP-VPN instance view, configure BGP route dampening (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] dampening 15 15 1000 2000 10000
```

default ipv4-unicast

Syntax **default ipv4-unicast**

undo default ipv4-unicast

View BGP view

Parameters None

Description Use the **default ipv4-unicast** command to enable the use of IPv4 unicast address family for all peers.

Use the **undo default ipv4-unicast** command to disable the use of IPv4 unicast address family for all peers.

The use of IPv4 unicast address family is enabled by default.

Examples # Enable IPv4 unicast address family for all neighbors.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default ipv4-unicast
```

default local-preference (BGP/BGP-VPN instance view)

Syntax **default local-preference** *value*

undo default local-preference

View BGP view/BGP-VPN instance view

Parameters *value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Using this command can affect BGP route selection.

Examples # In BGP view, set the default local preference to 180.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default local-preference 180
```

In BGP-VPN instance view, set the default local preference to 180 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default local-preference 180
```

default med (BGP/BGP-VPN instance view)

Syntax **default med** *med-value*

undo default med

View BGP view/BGP-VPN instance view

Parameters *med-value*: Default MED value, in the range 0 to 4294967295.

Description Use the **default med** command to specify a default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

Multi-exit discriminator (MED) is an external metric for routes. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with an identical destination but different next-hops from various external peers, it will select the best route depending on the MED value. In the case that all other conditions are the same, the system first selects the route with the smallest MED as the best external route.

Examples # In BGP view, configure the default MED as 25.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default med 25
```

In BGP-VPN instance view, configure the default MED as 25 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default med 25
```

default-route imported (BGP/BGP-VPN instance view)

Syntax **default-route imported**

undo default-route imported

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **default-route imported** command to allow default route redistribution into the BGP routing table.

Use the **undo default-route imported** command to disallow the redistribution.

By default, default route redistribution is not allowed.

Using the **default-route imported** command cannot redistribute default routes. To do so, use the **import-route** command.

Related commands: **import-route (BGP/BGP-VPN instance view)**.

Examples # In BGP view, allow default route redistribution from OSPF into BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] default-route imported
[Sysname-bgp] import-route ospf 1
```

In BGP-VPN instance view, enable redistributing default route from OSPF into BGP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] default-route imported
[Sysname-bgp-vpn1] import-route ospf 1
```

display bgp group

Syntax **display bgp group** [*group-name*]

View Any view

Parameters *group-name*: Peer group name, a string of 1 to 47 characters.

Description Use the **display bgp group** command to display the information of the peer group.

Examples # Display the information of the peer group **aaa**.

```
<Sysname> display bgp group aaa
 BGP peer-group is aaa
 remote AS 200
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer            V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  2.2.2.1         4   200        0        0     0       0 00:00:35 Active
```

Table 215 Description on the fields of the display bgp group command

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS	AS number of peer group
type	Type of the BGP peer group: IBGP or EBGP
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value

Table 215 Description on the fields of the display bgp group command

Field	Description
Configured hold timer value	Holdtime interval
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum time between advertisement runs
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer
Members	Detailed information of the members in the peer group
Peer	IPv4 address of the peer
V	BGP version running on peers
AS	AS number of the peers
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine of peer

display bgp network

Syntax **display bgp network**

View Any view

Parameters None

Description Use the **display bgp network** command to display routing information advertised with the **network** command.

Examples # Display routing information that has been advertised.

```
<Sysname> display bgp network

  BGP Local Router ID is 10.1.4.2.
  Local AS Number is 400.
  Network          Mask            Route-policy        Short-cut

  100.1.2.0        255.255.255.0
  100.1.1.0        255.255.255.0                       Short-cut
```

Table 216 Description on the fields of the display bgp network command

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address

Table 216 Description on the fields of the display bgp network command

Field	Description
Mask	Mask
Route-policy	Routing policy
Short-cut	Short-cut route

display bgp paths

Syntax **display bgp paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp paths** command to display information about BGP paths.

Examples # Display information about BGP paths matching the AS path regular expression.

```
<Sysname> display bgp paths ^200

    Address       Hash    Refcount  MED         Path/Origin
    0x5917100     11      1                     200 300i
```

Table 217 Description on the fields of the display bgp paths command

Field	Description	
Address	Route address in local database, in dotted hexadecimal notation	
Hash	Hash index	
Refcount	Count of routes that referenced the path	
MED	MED of the path	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means.

display bgp peer

Syntax **display bgp peer** [*ip-address* { **log-info** | **verbose** } | *group-name* **log-info** | **verbose**]

View Any view

Parameters *ip-address*: IP address of an peer to be displayed, in dotted decimal notation.

group-name: Name of a peer group to be displayed, a string of 1 to 47 characters.

log-info: Displays the log information of the specified peer.

verbose: Displays the detailed information of the peer/peer group.

Description Use the **display bgp peer** command to display peer/peer group information.

Examples # Display the detailed information of the peer 10.110.25.20.

```
<Sysname> display bgp peer 10.110.25.20 verbose

         Peer: 10.110.25.20 Local: 2.2.2.2
         Type: EBGP link
         BGP version 4, remote router ID 1.1.1.1
         BGP current state: Established, Up for 00h01m51s
         BGP current event: RecvKeepalive
         BGP last state: OpenConfirm
         Port:  Local - 1029     Remote - 179
         Configured: Active Hold Time: 180 sec   Keepalive Time: 60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer support bgp multi-protocol extended
         Peer support bgp route refresh capability
         Address family IPv4 Unicast: advertised and received

 Received: Total 5 messages, Update messages 1
 Sent: Total 4 messages, Update messages 0
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Minimum time between advertisement runs is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 Peer Preferred Value: 0

 Routing policy configured:
 No routing policy is configured
```

Table 218 Description on the fields of the display bgp peer command

Field	Description
Peer	IP address of the peer
Local	Local router ID
Type	Peer type: Internal as IBGP peers and External as EBGP peers.
BGP version	BGP protocol version
remote router ID	Router ID of the peer
BGP current state	Current state of the peer
BGP current event	Current event of the peer
BGP last state	Last state of the peer
Port	Port number of local router and its peer
Configured: Active Hold Time	Local holdtime interval
Keepalive Time	Local keepalive interval
Received: Active Hold Time	Remote holdtime interval
Negotiated: Active Hold Time	Negotiated holdtime interval

Table 218 Description on the fields of the display bgp peer command

Field	Description
Peer optional capabilities	Optional capabilities supported by the peer, including BGP multiple extension and routing refresh.
Address family IPv4 Unicast	Routes are advertised and received in the form of IPv4 unicast
Received	Total numbers of received packets and updates
Sent	Total numbers of sent packets and updates
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
Minimum time between advertisement runs	Minimum time between route advertisements
Optional capabilities	Optional capabilities enabled by the peer
Peer Preferred Value	Preferred value specified for the routes from the peer
Routing policy configured	Local routing policy

display bgp routing-table

Syntax **display bgp routing-table** [*ip-address* [{ *mask* | *mask-length* } [**longer-prefixes**]]]

View Any view

Parameters *ip-address*: Destination IP address.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-prefixes: Matches the longest prefix.

Description Use the **display bgp routing-table** command to display specified BGP routing information in the BGP routing table.

Examples # Display BGP routing table information.

```
<Sysname> display bgp routing-table

 Total Number of Routes: 1

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  40.40.40.0/24     20.20.20.1                              0       200 300i
```

Table 219 Description on the fields of the display bgp routing command

Field	Description
Total Number of Routes	Total Number of Routes

Table 219 Description on the fields of the display bgp routing command

Field	Description	
BGP Local router ID	BGP Local router ID	
Status codes	Status codes:	
	* - valid	
	> - best	
	d - damped	
	h - history	
	i - internal (IGP)	
	s - summary suppressed (suppressed)	
	S - Stale	
Origin	i - IGP (originated in the AS)	
	e - EGP (learned through EGP)	
	? - incomplete (learned by other means)	
Network	Destination network address	
Next Hop	Next hop IP address	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
PrefVal	Preferred value of the route	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
PrefVal	Preferred value	
Ogn	Origin attribute of the route, one of the following values:	
	i	Indicates that the route is interior to the AS. Summary routes and the routes configured using the **network** command are considered IGP routes.
	e	Indicates that the route is learned via the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of the route is unknown and the route is learned by other means.

display bgp routing-table as-path-acl

Syntax **display bgp routing-table as-path-acl** *as-path-acl-number*

View Any view

Parameters *as-path-acl-number*: Displays routing information permitted by the AS path ACL, which is specifies with a number from 1 to 256.

Description Use the **display bgp routing as-path-acl** command to display BGP routes permitted by an as-path ACL.

Examples # Display BGP routes permitted by AS path ACL 1.

```
<Sysname> display bgp routing-table as-path-acl 1

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop        MED        LocPrf      PrefVal Path/Ogn

*>  40.40.40.0/24     30.30.30.1     0                     0      300i
<Sysname> display bgp routing-table

 Total Number of Routes: 2
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network         NextHop        MED      ocPrf      PrefVal Path/Ogn

 *>  9.1.1.0/24     10.1.1.1                            0      65001 100i
 *>  10.1.5.0/24    10.1.1.1                            0      65001
                                                               65004i

<Sysname> display bgp routing-table as-path-acl 1

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network         NextHop      MED       LocPrf    PrefVal Path/Ogn

 *>  10.1.5.0/24     10.1.1.1                          0       65001
                                                               65004i
```

Refer to Table 219 for description on the fields above.

display bgp routing-table cidr

Syntax **display bgp routing-table cidr**

View Any view

Parameters None

Description Use the **display bgp routing-table cidr** command to display BGP CIDR (Classless Inter-Domain Routing) routing information.

Examples # Display BGP CIDR routing information.

```
<Sysname> display bgp routing-table cidr

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network          NextHop         MED        LocPrf     PrefVal Path/Ogn

*>  40.40.40.0/24    30.30.30.1      0                     0       300i
```

Refer to Table 219 for description on the above fields.

display bgp routing-table community

Syntax **display bgp routing-table community** [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View Any view

Parameters *aa:nn*: Community number. Both aa and nn are in the range 0 to 65535.

&<1-13>: Argument before it can be entered up to 13 times.

no-advertise: Displays BGP routes that are not advertised to any peer.

no-export: Displays routes that are not advertised outside the AS. With a confederation configured, it displays routes that are not advertised outside the confederation, but can be advertised to other sub ASs in the confederation.

no-export-subconfed: Displays routes that are neither advertised outside the AS nor to other sub ASs in a configured confederation.

whole-match: Displays the exactly matched routes.

Description Use the **display bgp routing community** command to display BGP routing information with the specified BGP community.

Examples # Display routing information with the specified BGP community.

```
<Sysname> display bgp routing-table community 11:22

 BGP Local router ID is 10.10.10.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  10.10.10.0/24     0.0.0.0         0                   0      i
 *>  40.40.40.0/24      20.20.20.1                             0       200 300i
```

Refer to Table 219 for description on the fields above.

display bgp routing-table community-list

Syntax **display bgp routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View Any view

Parameters *basic-community-list-number*: Specifies a basic community-list number from 1 to 99.

adv-community-list-number: Specifies an advanced community-list number from 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list*.

&<1-16>: Specifies the argument before it can be entered up to 16 times.

Description Use the **display bgp routing-table community-list** command to display BGP routing information matching the specified BGP community list.

Examples # Display BGP routing information matching BGP community list 100.

```
<Sysname> display bgp routing-table community-list 100
 BGP Local router ID is 1.2.3.4
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed,
 Origin codes: i - IGP, e - EGP, ? - incomplete
      Network            NextHop        Metric     LocPrf    PrefVal Path

 *>   3.3.3.0/30         1.2.3.4                              0       ?
 *>   4.4.0.0/20         1.2.3.4                              0       ?
 *>   4.5.6.0/26         1.2.3.4                              0       ?


 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn

 *>  30.30.30.0/24     0.0.0.0       0                    0       i
 *>  40.40.40.0/24     0.0.0.0       0                    0       i
```

Refer to Table 219 for description on the fields above.

display bgp routing-table dampened

Syntax **display bgp routing-table dampened**

View Any view

Parameters None

Description Use the **display bgp routing-table dampened** command to display dampened BGP routes.

Examples # Display dampened BGP routes.

```
<Sysname> display bgp routing-table dampened
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            From             Reuse     Path/Origin
 *d  77.0.0.0           12.1.1.1         00:29:20  100?
```

Table 220 Description on the fields of the display bgp routing-table dampened command

Field	Description
From	IP address from which the route was received
Reuse	Reuse time of the route

Refer to Table 219 for description on the other fields above.

display bgp routing-table dampening parameter

Syntax **display bgp routing-table dampening parameter**

View Any view

Parameters None

Description Use the **display bgp routing-table dampening parameter** command to display BGP route dampening parameters.

Related commands: **dampening (BGP/BGP-VPN instance view)**.

Examples # Display BGP route dampening parameters.

```
<Sysname> display bgp routing-table dampening parameter
 Maximum Suppress Time(in second) : 3069
 Ceiling Value                    : 16000
 Reuse Value                      : 750
 HalfLife Time(in  second)        : 900
 Suppress-Limit                   : 2000
```

Table 221 Description on the fields of the display bgp routing-table dampening parameter command

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Limit for a route to be desuppressed
HalfLife Time	Half-life time of active routes
Suppress-Limit	Limit for a route to be suppressed

display bgp routing-table different-origin-as

Syntax **display bgp routing-table different-origin-as**

View Any view

Parameters None

Description Use the **display bgp routing-table different-origin-as** command to display BGP routes originating from different autonomous systems.

Examples # Display BGP routes originating from different ASs.

```
<Sysname> display bgp routing-table different-origin-as
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  55.0.0.0         12.1.1.1       0                   0       100?
 *                   14.1.1.2       0                   0       300?
```

Refer to Table 219 for description on the fields above.

display bgp routing-table flap-info

Syntax **display bgp routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ip-address* [{ *mask* | *mask-length* } [**longer-match**]]]

View Any view

Parameters *as-regular-expression*: Displays route flap information that matches the AS path regular expression.

as-path-acl-number: Displays route flap information matching the AS path ACL. The number is in the range 1 to 256.

ip-address: Destination IP address.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

longer-match: Matches the longest prefix.

Description Use the **display bgp routing-table flap-info** command to display BGP route flap statistics. If no parameter is specified, this command displays all BGP route flap statistics.

Examples # Display BGP route flap statistics.

```
<Sysname> display bgp routing-table flap-info

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network        From        Flaps  Duration   Reuse     Path/Origin

 *>  55.0.0.0       12.1.1.1    2      00:00:16             100?
 *d  77.0.0.0       12.1.1.1    5      00:34:02   00:27:08  100?
```

Table 222 Description on the fields of the display bgp routing flap-info command

Field	Description
From	Source IP address of the route
Flaps	Number of routing flaps
Duration	Duration time of the flap route
Reuse	Reuse time of the flap route

Refer to Table 219 for description on the other fields above.

display bgp routing-table peer

Syntax **display bgp routing-table peer** *ip-address* { **advertised-routes** | **received-routes** } [*network-address* [*mask* | *mask-length*] | **statistic**]

View Any view

Parameters *ip-address*: IP address of a peer.

advertised-routes: Displays routing information advertised to the specified peer.

received-routes: Displays routing information received from the specified peer.

network-address: IP address of the destination network.

mask: Mask of the destination network, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

statistic: Displays route statistics.

Description Use the **display bgp routing-table peer** command to display BGP routing information advertised to or received from the specified BGP peer.

Related commands: **display bgp peer**.

Examples # Display BGP routing information advertised to BGP peer 20.20.20.1.

```
<Sysname> display bgp routing-table peer 20.20.20.1 advertised-routes

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network            NextHop         MED        LocPrf     PrefVal Path/Ogn

 *>  30.30.30.0/24     0.0.0.0        0                     0       i
 *>  40.40.40.0/24     0.0.0.0        0                     0       i
```

Refer to Table 219 for description on the fields above.

display bgp routing-table regular-expression

Syntax **display bgp routing-table regular-expression** *as-regular-expression*

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp routing-table regular-expression** command to display BGP routing information matching the specified AS regular expression.

Examples # Display BGP routing information matching AS regular expression 300$.

```
<Sysname> display bgp routing-table regular-expression 300$

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
     Network           NextHop       MED        LocPrf    PrefVal Path/Ogn

 *>  40.40.40.0/24     30.30.30.1    0                    0       300i
```

Refer to Table 219 for description on the fields above.

display bgp routing-table statistic

Syntax **display bgp routing-table statistic**

View Any view

Parameters None

Description Use the **display bgp routing-table statistic** command to display BGP routing statistics.

Examples # Display BGP routing statistics.

```
<Sysname> display bgp routing-table statistic

 Total Number of Routes: 4
```

Table 223 Description on the fields of the display bgp routing-table statistic command

Field	Description
Total number of routes	Total number of routes

ebgp-interface-sensitive

Syntax **ebgp-interface-sensitive**

undo ebgp-interface-sensitive

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **ebgp-interface-sensitive** command to enable the clearing of EBGP session on any interface that becomes down.

Use the **undo ebgp-interface-sensitive** command to disable the function.

This function is enabled by default.

Examples # In BGP view, enable the clearing of EBGP session on any interface that becomes down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ebgp-interface-sensitive
```

In BGP-VPN instance view, enable the clearing of EBGP session on any interface that becomes down (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] ebgp-interface-sensitive
```

filter-policy export (BGP/BGP-VPN instance view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View BGP view/BGP-VPN instance view

Parameters *acl-number*: Number of an ACL used to filter outgoing redistributed routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter outgoing redistributed routing information, a string of 1 to 19 characters.

direct: Filters direct routes.

isis *process-id*: Filters outgoing routes redistributed from an ISIS process. The ID is in the range 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from the OSPF process with an ID from 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The ID is in the range 1 to 65535.

static: Filters static routes.

If no routing protocol is specified, all outgoing routes are filtered.

Description Use the **filter-policy export** command to filter outgoing redistributed routes and only the routes permitted by the specified filter can be advertised.

Use the **undo filter-policy export** command to remove the filtering.

If no routing protocol is specified, the filtering applies to all outgoing redistributed routes.

By default, the filtering is not configured.

Examples # In BGP view, reference ACL 2000 to filter all outgoing redistributed routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 export
```

In BGP-VPN instance view, reference ACL 2000 to filter all outgoing redistributed routes (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 export
```

filter-policy import (BGP/BGP-VPN instance view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View BGP view/BGP-VPN instance view

Parameters *acl-number*: Number of an ACL used to filter incoming routing information, ranging from 2000 to 3999.

ip-prefix-name: Name of an IP prefix list used to filter incoming routing information, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to configure the filtering of incoming routing information.

Use the **undo filter-policy import** command to remove the filtering.

By default, incoming routing information is not filtered.

Examples # In BGP view, reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] filter-policy 2000 import
```

In BGP-VPN instance view, reference ACL 2000 to filter incoming routing information (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] filter-policy 2000 import
```

graceful-restart (BGP view)

Syntax **graceful-restart**

undo graceful-restart

View BGP view

Parameters None

Description Use the **graceful-restart** command to enable BGP Graceful Restart capability.

Use the **undo graceful-restart** command to disable BGP Graceful Restart capability.

By default, BGP Graceful Restart capability is disabled.

When a GR-capable BGP speaker restarts, the address family to which the speaker belongs can still maintain the forwarding state and send the End-Of-RIB marker, but the BGP speaker may not maintain its forwarding table.

Examples # Enable the Graceful Restart capability for BGP process 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart
```

graceful-restart timer restart

Syntax **graceful-restart timer restart** *timer*

undo graceful-restart timer restart

View BGP view

Parameters *timer*: Maximum time for a peer to reestablish a BGP session, in the range 3 to 600 seconds.

Description Use the **graceful-restart timer restart** command to configure the maximum time for a peer to reestablish a BGP session.

Use the **undo graceful-restart timer restart** command to restore the default.

By default, the maximum time for a peer to reestablish a BGP session is 150 seconds.

Examples # Configure the maximum time for a peer to reestablish a BGP session as 300 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer restart 300
```

graceful-restart timer wait-for-rib

Syntax **graceful-restart timer wait-for-rib** *timer*

undo graceful-restart timer wait-for-rib

View BGP view

Parameters *timer*: Time to wait for the End-of-RIB marker, in the range 3 to 300 seconds.

Description Use the **graceful-restart timer wait-for-rib** command to configure the time to wait for the End-of-RIB marker.

Use the **undo graceful-restart timer wait-for-rib** command to restore the default.

By default, the time to wait for the End-of-RIB marker is 180 seconds.

- *After a BGP session has been successfully (re)established, the End-of-RIB marker must be received within the time specified with this command.*
- *Using this command can speed up route convergence.*

Examples # Set the time to wait for the End-of-RIB marker to 100 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] graceful-restart timer wait-for-rib 100
```

group (BGP/BGP-VPN instance view)

Syntax **group** *group-name* [**external** | **internal**]

undo group *group-name*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

external: Creates an EBGP peer group, which can be the group of another sub AS in a confederation.

internal: Creates an IBGP peer group; not supported in BGP-VPN instance view.

Description Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group is created if neither **internal** nor **external** is specified.

Examples # In BGP view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 200
[Sysname-bgp] peer 10.1.1.1 group test
[Sysname-bgp] peer 10.1.2.1 group test
```

In BGP-VPN instance view, create an EBGP peer group **test** with AS number 200, and add EBGP peers 10.1.1.1 and 10.1.2.1 into the group (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 200
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
[Sysname-bgp-vpn1] peer 10.1.2.1 group test
```

import-route (BGP/BGP-VPN instance view)

Syntax **import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View BGP view/BGP-VPN instance view

Parameters *protocol*: Redistributes routes from the specified routing protocol, which can be **direct**, **isis**, **ospf**, **rip**, or **static** at present.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isis**, **ospf**, or **rip**.

med-value: Specifies the MED value to be applied to redistributed routes, ranging from 0 to 4294967295. If the argument is not specified, the cost of the redistributed route is used as its MED in the BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description Use the **import-route** command to configure BGP to redistribute routes from a specified routing protocol and advertise redistributed routes.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

By default, BGP does not redistribute routes from other protocols.

The ORIGIN attribute of routes redistributed with the **import-route** command is incomplete.

Examples # In BGP view, redistribute routes from RIP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] import-route rip
```

In BGP-VPN instance view, redistribute routes from RIP (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] import-route rip
```

log-peer-change

Syntax **log-peer-change**

undo log-peer-change

View BGP view

Parameters None

Description Use the **log-peer-change** command to enable the global BGP logging on peers going up and down.

Use the **undo log-peer-change** command to disable the function.

By default, the function is enabled.

Examples # Enable BGP logging on peers going up and down.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] log-peer-change
```

network (BGP/BGP-VPN instance view)

Syntax **network** *ip-address* [*mask* | *mask-length*] [**short-cut** | **route-policy** *route-policy-name*]

undo network *ip-address* [*mask* | *mask-length*] [**short-cut**]

View BGP view/BGP-VPN instance view

Parameters *ip-address*: Destination IP address.

mask: Mask of the network address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

short-cut: Specifies the route to use the local preference. If the route is an EBGP route whose preference is higher than the local one, using this keyword can configure the EBGP route to use the local preference, so the route is hard to become the optimal route.

route-policy-name: Routing policy applied to the route. The name is a string of 1 to 19 characters.

Description Use the **network** command to inject a network to the local BGP routing table.

Use the **undo network** command to remove a network from the routing table.

By default, no network route is injected.

Note that:

- The network route must be in the local IP routing table, and using a routing policy makes route management more flexible.
- The route injected to the BGP routing table using the **network** command has the ORIGIN attribute as IGP.

Examples # In BGP view, inject the network segment 10.0.0.0/16.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] network 10.0.0.0 255.255.0.0
```

In BGP-VPN instance view, inject the network segment 10.0.0.0/16 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] network 10.0.0.0 255.255.0.0
```

peer advertise-community (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to disable the community attribute advertisement to a peer/peer group.

By default, no community attribute is advertised to any peer group/peer.

Related commands: **ip community-list**, **if-match community**, **apply community**.

Examples # In BGP view, advertise the community attribute to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-community
```

In BGP-VPN instance view, advertise the community attribute to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer advertise-ext-community (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **advertise-ext-community**

undo peer { *group-name* | *ip-address* } **advertise-ext-community**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to disable the advertisement.

By default, no extended community attribute is advertised to a peer/peer group.

For related information, refer to "ip extcommunity-list" on page 1205, "if-match extcommunity" on page 1199 and "apply extcommunity" on page 1190.

Examples # In BGP view, advertise the extended community attribute to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test advertise-ext-community
```

In BGP-VPN view, advertise the extended community attribute to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test advertise-community
```

peer allow-as-loop (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

number: Specifies the repeating times of the local AS number, in the range 1 to 10. The default number is 1.

Description Use the **peer allow-as-loop** command to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to remove the configuration.

By default, the local AS number is allowed.

Related commands: **display bgp routing-table peer**.

Examples # In BGP view, configure the repeating times of the local AS number as 2 for routes from peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 allow-as-loop 2
```

In BGP-VPN instance view, configure the repeating times of the local AS number as 2 for routes from peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 allow-as-loop 2
```

peer as-number (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **as-number** *as-number*

undo peer *group-name* **as-number**

undo peer *ip-address*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer or peer group, in the range 1 to 65535.

Description Use the **peer as-number** command to specify the AS number for a peer/peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # In BGP view, specify the AS number of the peer group **test** as 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
```

In BGP-VPN instance view, specify the AS number of the peer group **test** as 100 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
```

peer as-path-acl (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *as-path-acl-number* { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-path-acl-number: AS path ACL number, in the range 1 to 256.

export: Filters outgoing routes.

import: Filters incoming routes.

Description Use the **peer as-path-acl** command to configure the filtering of routes incoming from or outgoing to a peer/peer group based on a specified AS path ACL.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path ACL filtering is configured.

Related commands: **ip as-path** *acl*, **if-match as-path** and **apply as-path**.

Examples # In BGP view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-path-acl 1 export
```

In BGP-VPN instance view, reference the AS path ACL 1 to filter routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-path-acl 1 export
```

peer capability-advertise conventional

Syntax **peer** { *group-name* | *ip-address* } **capability-advertise conventional**

undo peer { *group-name* | *ip-address* } **capability-advertise conventional**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer capability-advertise conventional** command to disable BGP multi-protocol extension and route refresh for a peer/peer group.

Use the **undo peer capability-advertise** command to enable BGP multi-protocol extension and route refresh for a peer/peer group.

By default, BGP multi-protocol extension and route refresh are enabled.

Examples # In BGP view, disable multi-protocol extension and route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise conventional
```

peer capability-advertise route-refresh

Syntax **peer** { *group-name* | *ip-address* } **capability-advertise route-refresh**

undo peer { *group-name* | *ip-address* } **capability-advertise route-refresh**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable the BGP route refresh capability.

Use the **undo peer capability-advertise route-refresh** command to disable the capability.

The capability is enabled by default.

Examples # In BGP view, enable BGP route refresh for peer 160.89.2.33.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 160.89.2.33 as-number 100
[Sysname-bgp] peer 160.89.2.33 capability-advertise route-refresh
```

In BGP-VPN instance view, enable BGP route refresh for peer 160.89.2.33 (The VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 160.89.2.33 as-number 100
[Sysname-bgp-vpn1] peer 160.89.2.33 capability-advertise route-refresh
```

peer connect-interface (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **connect-interface** *interface-type interface-number*

undo peer { *group-name* | *ip-address* } **connect-interface**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string 1 to 47 characters.

ip-address: IP address of a peer.

interface-type interface-number: Specifies the type and number of the interface.

Description Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to a peer/peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the BGP peer/peer group as the source interface for establishing a TCP connection to the peer/peer group.

Note that:

To establish multiple BGP connections to another BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router because the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples # In BGP view, specify loopback 0 as the source interface for routing updates to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test connect-interface loopback 0
```

In BGP-VPN instance view, specify loopback 0 as the source interface for routing updates to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test connect-interface loopback 0
```

peer default-route-advertise (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ip-address* } **default-route-advertise**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

Description Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable default route advertisement to a peer/peer group.

By default, no default route is advertised to a peer/peer group.

With this command used, the router unconditionally sends a default route with the next hop being itself to the peer/peer group regardless of whether the default route is available in the routing table.

Examples # In BGP view, advertise a default route to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test default-route-advertise
```

In BGP-VPN instance view, advertise a default route to peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test default-route-advertise
```

peer description (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **description** *description-text*

undo peer { *group-name* | *ip-address* } **description**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer/peer group.

Create a peer/peer group before configuring a description for it.

Related commands: **display bgp peer**.

Examples # In BGP view, configure the description information of the peer group test as ISP1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test description ISP1
```

In BGP-VPN instance view, configure the description information of the peer group test as ISP1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test description ISP1
```

peer ebgp-max-hop (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *group-name* | *ip-address* } **ebgp-max-hop**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

hop-count: Maximum hop count, in the range 1 to 255. The default is 64.

Description Use the **peer ebgp-max-hop** command to allow establishing an EBGP connection with a peer/peer group that is on an indirectly connected network.

Use the **undo peer ebgp-max-hop** command to restore the default.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum route count of the EBGP connection.

Examples # In BGP view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ebgp-max-hop
```

In BGP-VPN instance view, allow establishing the EBGP connection with the peer group **test** that is on an indirectly connected network (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ebgp-max-hop
```

peer enable (BGP view)

Syntax **peer** *ip-address* **enable**

undo peer *ip-address* **enable**

View BGP view

Parameters *ip-address*: IP address of a peer.

Description Use the **peer enable** command to enable the specified peer.

Use the **undo peer enable** command to disable the specified peer.

By default, the BGP peer is enabled.

If a peer is disabled, the router will not exchange routing information with the peer.

Examples # Disable peer 18.10.0.9.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 18.10.0.9 group group1
[Sysname-bgp] undo peer 18.10.0.9 enable
```

peer fake-as (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **fake-as** *as-number*

undo peer { *group-name* | *ip-address* } **fake-as**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

*The **peer fake-as** command is only applicable to an EBGP peer or peer group.*

Examples # In BGP view, configure a fake AS number of 200 for the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test fake-as 200
```

In BGP-VPN instance view, configure a fake AS number of 200 for the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test fake-as 200
```

peer filter-policy (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** [*acl-number*] { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Applies the filter-policy to routes advertised to the peer/peer group.

import: Applies the filter-policy to routes received from the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Related commands: **peer as-path-acl (BGP/BGP-VPN instance view)**.

Examples # In BGP view, apply the ACL 2000 to filter routes advertised to the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test filter-policy 2000 export
```

In BGP-VPN instance view, apply the ACL 2000 to filter routes advertised to the peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test filter-policy 2000 export
```

peer group (BGP/BGP-VPN instance view)

Syntax **peer** *ip-address* **group** *group-name* [**as-number** *as-number*]

undo peer *ip-address* **group** *group-name*

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

as-number: AS number of the peer, in the range 1 to 65535.

Description Use the **peer group** command to add a peer to a peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, no peer is added into a peer group.

Examples # In BGP view, add the peer 10.1.1.1 to the EBGP peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] peer test as-number 2004
[Sysname-bgp] peer 10.1.1.1 group test
```

In BGP-VPN view, add the peer 10.1.1.1 to the EBGP peer group test (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] group test external
[Sysname-bgp-vpn1] peer test as-number 2004
[Sysname-bgp-vpn1] peer 10.1.1.1 group test
```

peer ignore (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **ignore**

undo peer { *group-name* | *ip-address* } **ignore**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer ignore** command to disable session establishment with a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, session establishment with a peer or peer group is allowed.

After the **peer ignore** command is executed, the system disables the session with the specified peer or peer group and clears all the related routing information. For a peer group, this means all sessions with the peer group will be tore down.

Examples # In BGP view, disable session establishment with peer 10.10.10.10.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.10.10.10 ignore
```

In BGP-VPN instance view, disable session establishment with peer 10.10.10.10 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.10.10.10 ignore
```

peer ip-prefix

Syntax **peer** { *group-name* | *ip-address* } **ip-prefix** *ip-prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

ip-prefix-name: IP prefix list name, a string of 1 to 19 characters.

export: Applies the filter to routes advertised to the specified peer/peer group.

import: Applies the filter to routes received from the specified peer/peer group.

Description Use the **peer ip-prefix** command to reference an IP prefix list to filter routes received from or advertised to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no IP prefix list is specified.

Examples # In BGP view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test ip-prefix list1 export
```

In BGP-VPN view, use the IP prefix list **list 1** to filter routes advertised to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test ip-prefix list1 export
```

peer keep-all-routes (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **keep-all-routes**

undo peer { *group-name* | *ip-address* } **keep-all-routes**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer keep-all-routes** command to save original routing information from a peer or peer group, even routes that failed to pass the inbound policy (if configured).

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples # In BGP view, save routing information from peer 131.100.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.100.1.1 as-number 200
[Sysname-bgp] peer 131.100.1.1 keep-all-routes
```

In BGP-VPN instance view, save routing information from peer 131.100.1.1(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.100.1.1 as-number 200
[Sysname-bgp-vpn1] peer 131.100.1.1 keep-all-routes
```

peer log-change (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **log-change**

undo peer { *group-name* | *ip-address* } **log-change**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information for a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # In BGP view, enable the logging of session state and event information for peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test log-change
```

In BGP-VPN instance view, enable the logging of session state and event information for peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test log-change
```

peer next-hop-local (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View BGP view /BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer next-hop-local** command to specify the router as the next hop for routes to a peer/peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

By default, routes advertised to an EBGP peer/peer group take the local router as the next hop, while routes to an IBGP peer/peer group do not take the local router as the next hop.

Examples # In BGP view, set the next hop of routes advertised to peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test next-hop-local
```

In BGP-VPN instance view, set the next hop of routes advertised to peer group **test** to the router itself (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test next-hop-local
```

peer password

Syntax **peer** { *group-name* | *ip-address* } **password** { **cipher** | **simple** } *password*

undo peer { *group-name* | *ip-address* } **password**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

cipher: Displays the configured password in cipher text format.

simple: Displays the configured password in plain text format.

password: Password, a string of 1 to 80 characters when keyword **simple** is used, or when keyword **cipher** is included and plain text password is input; a string of 24 or 108 characters when cipher text password and the keyword **cipher** are used.

Description Use the **peer password** command to configure BGP to perform MD5 authentication when a TCP connection is being established with a peer/peer group.

Use the **undo peer password** command to disable the function.

By default, no MD5 authentication is performed for TCP connection establishment.

Once MD5 authentication is enabled, both parties must be configured with the same authentication mode and password. Otherwise, the TCP connection will not be set up.

Examples # In BGP view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 10.1.100.1 password simple aabbcc
```

In BGP-VPN instance view, perform MD5 authentication on the TCP connection set up between the local router 10.1.100.1 and the peer router 10.1.100.2(the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.2 password simple aabbcc
```

Perform the similar configuration on the peer.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 10.1.100.1 password simple aabbcc
```

peer preferred-value (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **preferred-value** *value*

undo peer { *group-name* | *ip-address* } **preferred-value**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

value: Preferred value, in the range 0 to 65535.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default value.

The default preferred value is 0.

Routes learned from a peer have an initial preferred value.

Among multiple routes that have the same destination/mask and are learned from different peers, the one with the biggest preferred value is selected as the route to the network.

Note that:

If you both reference a routing policy and use the **peer** { *group-name* | *ip-address* } **preferred-value** *value* command to set a preferred value for routes from a peer, the routing policy sets a specified non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value specified in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to **"peer group (BGP/BGP-VPN instance view)" on page 994**, **"peer route-policy (BGP/BGP-VPN instance view)" on page 1002** { **export** | **import** } in this document, and **"apply preferred-value" on page 1194**

Examples # In BGP view, configure the preferred value as 50 for routes from peer 131.108.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 131.108.1.1 preferred-value 50
```

In BGP-VPN instance view, configure the preferred value as 50 for routes from peer 131.108.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 131.108.1.1 preferred-value 50
```

peer public-as-only (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer public-as-only** command to not keep private AS numbers in BGP updates sent to a peer/peer group.

Use the **undo peer public-as-only** command to keep private AS numbers in BGP updates sent to a peer/peer group.

By default, BGP updates carry private AS numbers.

The command does not take effect if the BGP update has both public and private AS numbers. The range of private AS number is from 64512 to 65535.

Examples # In BGP view, carry no private AS number in BGP updates sent to the peer **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test public-as-only
```

In BGP-VPN instance view, carry no private AS number in BGP updates sent to the peer **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test public-as-only
```

peer reflect-client (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View BGP view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer reflect-client** command to configure the router as a router reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients (BGP view)** and **reflector cluster-id (BGP view)**.

Examples # In BGP view, configure the local device as a router reflector and specify the IBGP peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test reflect-client
```

peer route-limit (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-limit** *limit* [*percentage*]

undo peer { *group-name* | *ip-address* } **route-limit**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

limit: Upper limit of IP prefixes that can be received from the peer or peer group, in the range 1 to 10000.

percentage: If the number of received routes reaches the specified percentage of the upper limit, the system will generate alarm information. The percentage is in the range from 1 to 100. The default is 75.

Description Use the **peer route-limit** command to set the maximum number of routes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

The number is unlimited by default.

Examples # In BGP view, set the number of routes that can be received from peer 129.140.6.6 to 10000.

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] peer 129.140.6.6 as-number 110
[Sysname-bgp] peer 129.140.6.6 route-limit 10000
```

In BGP-VPN instance view, set the maximum number of routes that can be received from peer 129.140.6.6 to 10000 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 109
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 129.140.6.6 as-number 110
[Sysname-bgp-vpn1] peer 129.140.6.6 route-limit 10000
```

peer route-policy (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a string of 1 to 47 characters.

ip-address: IP address of a peer.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

export: Applies the routing policy to routes outgoing to the peer (or peer group).

import: Applies the routing policy to routes incoming from the peer (or peer group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no inbound/outbound routing policy is configured for the peer/peer group.

The **peer route-policy** command does not apply the **if-match interface** clause in the referenced routing policy. Refer to "route-policy" on page 1205 and "if-match interface" on page 1200

Examples # In BGP view, apply routing policy **test-policy** to routes outgoing to peer group **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test route-policy test-policy export
```

In BGP-VPN instance view, apply routing policy **test-policy** to routes outgoing to the peer group **test** (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test route-policy test-policy export
```

peer route-update-interval (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **route-update-interval** *seconds*

undo peer { *group-name* | *ip-address* } **route-update-interval**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

seconds: Minimum interval for sending the same update message. The range is 5 to 600 seconds.

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default value.

By default, the interval is 5 seconds for IBGP peers, and 30 seconds for EBGP peers.

Examples # In BGP view, specify the interval for sending the same update to peer group **test** as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test as-number 100
[Sysname-bgp] peer test route-update-interval 10
```

In BGP-VPN instance view, specify the interval for sending the same update to peer group **test** as 10 seconds (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test as-number 100
[Sysname-bgp-vpn1] peer test route-update-interval 10
```

peer substitute-as (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **substitute-as**

undo peer { *group-name* | *ip-address* } **substitute-as**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

Description Use the **peer substitute-as** command to replace the AS number of a peer/peer group in the AS_PATH attribute with the local AS number.

Use the **undo peer substitute-as** command to remove the configuration.

No AS number is replaced by default.

Examples # In BGP view, substitute local AS number for AS number of peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 substitute-as
```

In BGP-VPN instance view, substitute local AS number for AS number of peer 1.1.1.1 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer 1.1.1.1 substitute-as
```

peer timer (BGP/BGP-VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *group-name* | *ip-address* } **timer**

View BGP view/BGP-VPN instance view

Parameters *group-name*: Name of a peer group, a sting of 1 to 47 characters.

ip-address: IP address of a peer.

keepalive: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **peer timer** command to configure the keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

By default, the *keepalive* and *holdtime* are 60s and 180s respectively.

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer (BGP/BGP-VPN instance view)**.

Examples # In BGP view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer test timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure the keepalive interval and holdtime interval for peer group **test** as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] peer test timer keepalive 60 hold 180
```

preference (BGP/BGP-VPN instance view)

Syntax **preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View BGP view/BGP-VPN instance view

Parameters *external-preference*: Preference of EBGP route, in the range 1 to 255.

internal-preference: Preference of IBGP route, in the range 1 to 255. An IBGP is a route learned from another peer inside AS.

local-preference: Preference of local route, in the range 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. Using the routing policy can set preference for routes passing through it. For the routes filtered out, the default value applies.

Description Use the **preference** command to configure preferences for external, internal, and local routes.

Use the **undo preference** command to restore the default.

For *external-preference*, *internal-preference* and *local-preference*, the bigger the preference value is, the lower the preference is, and the default values are 255, 255, 130 respectively.

Examples # In BGP view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] preference 20 20 200
```

In BGP-VPN instance view, configure preferences for EBGP, IBGP and local routes as 20, 20 and 200 (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] preference 20 20 200
```

reflect between-clients (BGP view)

Syntax **reflect between-clients**

undo reflect between-clients

View BGP view

Parameters None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects the routes of a client to other clients. If the clients of a route reflector are fully meshed, you need disable route reflection between clients to reduce routing costs.

Related commands: **reflector cluster-id (BGP view)** and **peer reflect-client (BGP/BGP-VPN instance view)**.

Examples # Disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo reflect between-clients
```

reflector cluster-id (BGP view)

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View BGP view

Parameters *cluster-id*: Cluster ID of the route reflector, an integer from 1 to 4294967295 (the integer is translated into an IP address by the system) or an IP address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, each route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster. The router ID of the route reflector is the ID of the cluster. You can configure multiple route reflectors to improve the stability of the network. In this case, using this command can configure the identical cluster ID for all the route reflectors to avoid routing loops.

Related commands: **reflect between-clients (BGP view)** and **peer reflect-client (BGP/BGP-VPN instance view)**.

Examples # Set the cluster ID to 80.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] reflector cluster-id 80
```

refresh bgp

Syntax **refresh bgp** { **all** | *ip-address* | **group** *group-name* | **external** | **internal** } { **export** | **import** }

View User view

Parameters **all**: Soft-resets all BGP connections.

ip-address: Soft-resets the BGP connection to a peer.

group-name: Soft-resets connections to a peer group, name of which is a sting of 1 to 47 characters.

external: EBGP connection.

internal: IBGP connection.

export: Outbound soft reset.

import: Inbound soft reset.

Description Use the **refresh bgp** command to perform soft reset on specified BGP connections. Using this function can refresh the BGP routing table without tearing down BGP connections and apply a newly configured routing policy.

To perform BGP soft reset, all routers in the network must support route-refresh. If a router not supporting route-refresh exists in the network, you need to configure the **peer keep-all-routes** command to save all routing updates before performing soft reset.

Examples # Perform inbound BGP soft reset.

```
<Sysname> refresh bgp all import
```

reset bgp

Syntax **reset bgp** { **all** | *as-number* | *ip-address* [**flap-info**] | **group** *group-name* | **external** | **internal** }

View User view

Parameters **all**: Resets all BGP connections.

as-number: Resets BGP connections to peers in the AS.

ip-address: Specifies the IP address of a peer with which to reset the connection.

flap-info: Clears history information of routing flap.

group *group-name*: Specifies to reset connections with the specified BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp** command to reset specified BGP connections.

Examples # Reset all the BGP connections.

```
<Sysname> reset bgp all
```

reset bgp dampening

Syntax **reset bgp dampening** [*ip-address* [*mask* | *mask-length*]]

View User view

Parameters *ip-address*: Destination IP address of a route.

mask: Mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description Use the **reset bgp dampening** command to clear route dampening information and release suppressed routes.

Related commands: **dampening (BGP/BGP-VPN instance view)**, **display bgp routing-table dampened**.

Examples # Clear damping information of route 20.1.0.0/16 and release suppressed route.

```
<Sysname> reset bgp dampening 20.1.0.0 255.255.0.0
```

reset bgp flap-info

Syntax **reset bgp flap-info** [**regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number* | *ip-address* [*mask* | *mask-length*]]

View User view

Parameters *as-path-regexp*: Clears the flap statistics of routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics of routes matching an AS path ACL, number of which is in the range 1 to 256.

ip-address: Clears the flap statistics of a route.

mask: Network mask, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

Description Use the **reset bgp flap-info** command to clear the flap statistics of routes matching the specified filter.

The flap statistics of all the routes will be cleared if no parameter is specified.

Examples # Clear the flap statistics of all routes matching AS path ACL 10.

```
<Sysname> reset bgp flap-info as-path-acl 10
```

reset bgp ipv4 all

Syntax **reset bgp ipv4 all**

View User view

Parameters None

Description Use the **reset bgp ipv4 all** command to reset all the BGP connections of IPv4 unicast address family.

Examples # Reset all the BGP connections of IPv4 unicast address family.

```
<Sysname> reset bgp ipv4 all
```

router-id

Syntax **router-id** *router-id*

undo router-id

View BGP view

Parameters *router-id*: Router ID in IP address format.

Description Use the **router-id** command to specify a router ID.

Use the **undo router-id** command to remove a router ID.

To run BGP protocol, a router must have a router ID, which is an unsigned 32-bit integer, the unique ID of the router in the AS.

You can specify a router ID manually. If not, the system selects an IP address as the router ID. The selection sequence is the highest IP address among loopback interface addresses; if not available, then the highest IP address of interfaces. It is recommended to specify a loopback interface address as the router ID to enhance network reliability.

Only when the interface with the selected Router ID or the manual Router ID is deleted will the system select another ID for the router.

Examples # Specifies the Router ID as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

summary automatic

Syntax **summary automatic**

undo summary automatic

View BGP view/BGP-VPN instance view

Parameters None

Description Use the **summary automatic** command to enable automatic summarization for redistributed subnets.

Use the **undo summary automatic** command to disable automatic summarization.

By default, automatic summarization is disabled.

Note that:

- Neither the default route nor the routes imported using the **network** command can be summarized automatically.
- With this feature enabled, BGP limits the subnets redistribution from IGP to reduce the size of routing table.

Examples # In BGP view, enable automatic summarization.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] summary automatic
```

In BGP-VPN instance view, enable automatic summarization (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] summary automatic
```

synchronization (BGP view)

Syntax **synchronization**

undo synchronization

View BGP view

Parameters None

Description Use the **synchronization** command to enable the synchronization between the BGP and IGP routes.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

When a BGP router receives an IBGP route, it checks only whether the next hop is reachable by default. If the synchronization is enabled, the IBGP route is synchronized and advertised to EBGP peers only when the route is also advertised by IGP. Otherwise, the IBGP route cannot be advertised to EBGP peers.

Examples # Enable the synchronization between BGP and IGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] synchronization
```

timer (BGP/BGP-VPN instance view)

Syntax **timer keepalive** *keepalive* **hold** *holdtime*

undo timer

View BGP view/BGP-VPN instance view

Parameters *keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **timer** command to configure BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, BGP keepalive and holdtime intervals are 60s and 180s.

Note that:

- Timer configured using the **peer timer** command is preferred to the timer configured using this command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the BGP peers, while it becomes valid only after the corresponding BGP connections are reset.

Related commands: **peer timer (BGP/BGP-VPN instance view)**.

Examples # Configure keepalive interval and holdtime interval as 60s and 180s.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] timer keepalive 60 hold 180
```

In BGP-VPN instance view, configure keepalive interval and holdtime interval as 60s and 180s (the VPN has been created).

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1] timer keepalive 60 hold 180
```

73 BGP DEBUGGING COMMANDS

debugging bgp all

Syntax **debugging bgp** [*ipv4-address* | *ipv6-address*] **all**

undo debugging bgp [*ipv4-address* | *ipv6-address*] **all**

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **debugging bgp all** command to enable all BGP debugging.

Use the **undo debugging bgp all** command to disable all BGP debugging.

By default, all BGP debugging is disabled.

Note the following:

- This command enables all BGP debugging, which may cause heavy traffic and affect system performance; therefore, use this command only when necessary.
- Disable debugging once the debugging operation is complete.

Examples # Enable all BGP debugging while Device A and Device B are establishing an IBGP peer relationship with each other.

```
[Sysname-bgp]display this
#
bgp 100
 undo synchronization
 peer 10.1.1.2 as-number 100
#
======================
[Sysname-bgp] display this
#
bgp 100
 undo synchronization
 peer 10.1.1.1 as-number 100
#
```

// BGP configuration information

```
<Sysname> debugging bgp all
*Aug 24 15:31:55:316 2006 Sysname RM/6/RMDEBUG:
 BGP_TIMER: CR Timer Expired for Peer 10.1.1.2
*Aug 24 15:31:55:316 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is CRTimerExpired.
*Aug 24 15:31:55:316 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is Start.
*Aug 24 15:31:55:331 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from IDLE to CONNECT.
```

// Upon expiration of the connect timer, BGP initiated a connection with the peer.

```
*Aug 24 15:31:55:331 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is TransConnOpenFailed.
*Aug 24 15:31:55:331 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from CONNECT to ACTIVE.
*Aug 24 15:32:02:630 2006 Sysname RM/6/RMDEBUG:
         BGP.: 10.1.1.2 Send OPEN, Version: 4
         Local AS: 100, HoldTime: 180, Router ID: 10.1.1.1
         OPT Type:   2 (Capability)
         CAP Type:   1 (Multiprotocol)  CAP Len: 4
                                        IPv4-UNC (1/1)
         CAP Type:   2 (RouteRefresh)   CAP Len: 0

         Total CAPB Len    : 8
         Total OPT Len     : 10
         Total Message Len : 39
*Aug 24 15:32:02:630 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from ACTIVE to OPENSENT.
```

// After the connection is established, BGP sent an OPEN message to the peer.

```
*Aug 24 15:32:02:630 2006 Sysname RM/6/RMDEBUG:
         BGP.: 10.1.1.2 Recv OPEN Length: 39
         Version: 4, Local AS: 100, HoldTime : 180,
         BGP ID: 10.1.1.2, TotOptLen: 10

         OPT Type:   2 (Capability)     OPT Len: 8
         CAP Type:   1 (Multiprotocol)  CAP Len: 4
                                        IPv4-UNC (1/1)
         CAP Type:   2 (RouteRefresh)   CAP Len: 0
*Aug 24 15:32:02:630 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is ReceiveOpenMessage.
```

// BGP received an OPEN message from the peer

```
*Aug 24 15:32:02:646 2006 Sysname RM/6/RMDEBUG:
         BGP.: 10.1.1.2 Send KEEPALIVE
         Length 19
*Aug 24 15:32:02:646 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from OPENSENT to OPENCONFIRM.
%Aug 24 15:32:02:674 2006 Sysname RM/3/RMLOG:
 BGP.: 10.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.
*Aug 24 15:32:02:674 2006 Sysname RM/6/RMDEBUG:
         BGP.: 10.1.1.2 Recv KEEPALIVE
```

```
         Length: 19
*Aug 24 15:32:02:674 2006 Sysname RM/6/RMDEBUG:
 BGP.      : 10.1.1.2 Current event is RecvKeepAliveMessage.
*Aug 24 15:32:02:674 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.
```

// BGP has established the peer relationship successfully.

*The display above is the debugging information shown by executing the **debugging bgp all** command on Device A. If the peer relationship between two devices cannot be established, you can compare the above debugging information with the actual debugging information to locate the fault. For detailed descriptions on the specific messages, refer to the commands below.*

debugging bgp detail

Syntax **debugging bgp detail**

undo debugging bgp detail

View User view

Default Level 1: Monitor level

Parameters None

Description Use the **debugging bgp detail** command to enable detailed debugging for BGP.

Use the **undo debugging bgp detail** command to disable detailed debugging for BGP.

Enabling debugging may affect system performance; therefore, use this command only when necessary. Disable debugging once the debugging operation is complete.

By default, detailed debugging for BGP is disabled.

Table 224 Description on the fields of the debugging bgp detail command

Field	Description
BGP.xxx	BGP instance name
BGP can't get physical interface index for destination:*X.X.X.X*	BGP cannot get the physical interface index for destination *X.X.X.X*.
Fail to search Token for destination *X.X.X.X*	Token search for destination *X.X.X.X* failed.
Allocate token failed. destination= *X.X.X.X*,LspmErr=*X*	Failed to allocate Token: destination *X.X.X.X*, LSP error code X
There are *XX* routes allocate token failed at this time before	Failed to allocate Tokens for XX routes
Recv UPDATE with following RD *XXX*	Received an Update message with RD XXX

Table 224 Description on the fields of the debugging bgp detail command

Field	Description
Received New VPNv4 Route with Ext-Community NULL.Ignoring Route	Received a new VPNv4 route with Ext-Community as NULL and therefore ignored the route.
Received VPNv4 Packet But No Such Route In Loc Rib	Received a VPNv4 packet and there is no such a route in the local routing table
operation XX	Label operation code
Receive SMB UP backup requirement	Received a standby board startup event requesting an active/standby switchover
Receive routine backup requirement	Received a routine request for an active/standby switchover
Receive SMB down backup requirement	Received a standby board down event requesting an active/standby switchover

Examples # Enable detailed debugging for BGP when a BGP peer relationship is being established.

```
<Sysname> debugging bgp detail
*Aug 24 14:12:13:674 2006 Sysname RM/6/RMDEBUG:
BGP_L3VPN: Recv UPDATE with following RD 100:1 destination 11.1.1.1
- Received New VPNv4 Route with Ext-Community NULL..Ignoring Route
```

// BGP received an UPDATE message with RD 100:1, destination address 11.1.1.1. The Ext-Community of the new VPNv4 route is NULL and therefore the route was ignored.

```
DeLocRemCross: Deleting route From Target Instance.
```

// The route was deleted from the instance

debugging bgp event

Syntax **debugging bgp** [*ipv4-address* | *ipv6-address*] **event**

undo debugging bgp [*ipv4-address* | *ipv6-address*] **event**

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **debugging bgp event** command to enable event debugging for BGP.

Use the **undo debugging bgp event** command to disable event debugging for BGP.

The **debugging bgp event** command is used to enable BGP event debugging, which is mainly related to events triggering the BGP state machine transitions.

After this debugging is enabled, information about all the BGP state machine transitions and the events triggering these transitions will be displayed. If no BGP peer relationship can be established, you can enable this debugging to locate the fault. Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

By default, BGP event debugging is disabled.

Table 225 Description on the fields of the debugging bgp event command

Field	Description
Current event is *Eventname*	Name of the current event

Examples # Enable BGP event debugging when a BGP peer relationship is being established.

```
<Sysname> debugging bgp event
*Aug 24 14:12:13:674 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is CRTimerExpired.
*Aug 24 14:12:13:674 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from ACTIVE to CONNECT.
*Aug 24 14:12:14:690 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from CONNECT to ACTIVE.
*Aug 24 14:12:13:706 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from ACTIVE to OPENSENT.
*Aug 24 14:12:13:706 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is ReceiveOpenMessage.
```

// BGP received an OPEN message.

```
*Aug 24 14:12:13:706 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from OPENSENT to OPENCONFIRM.
```

// The state has changed from OPENSENT to OPENCONFIRM.

```
%Aug 24 14:12:13:728 2006 Sysname RM/3/RMLOG:
 BGP.: 10.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.
*Aug 24 14:12:13:728 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is RecvKeepAliveMessage.
*Aug 24 14:12:13:728 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 State is changed from OPENCONFIRM to ESTABLISHED.
<Sysname>
*Aug 24 14:12:44:696 2006 Sysname RM/6/RMDEBUG:
 BGP.: 10.1.1.2 Current event is RecvUpdateMessage.
```

// BGP has received an UPDATE message.

debugging bgp graceful-restart

Syntax **debugging bgp** [*ipv4-address* | *ipv6-address*] **graceful-restart**

undo debugging bgp [*ipv4-address* | *ipv6-address*] **graceful-restart**

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **debugging bgp graceful-restart** command to enable GR event debugging for BGP.

Use the **undo debugging bgp graceful-restart** command to disable GR event debugging for BGP.

After this debugging is enabled, the debugging information of the BGP GR operation will be displayed, including the currently triggered event, state transitions, receiving/sending of EOR messages, and peer IP address. If a fault occurs to the GR operation of BGP, you can display the debugging information for fault location.

Enabling debugging may affect system performance; therefore, use the command only when necessary and disable debugging once the debugging operation is complete.

By default, this debugging is disabled.

Examples # Enable BGP GR event debugging on the BGP GR Helper when the neighbor performs an active/standby switchover.

```
<Sysname> debugging bgp graceful-restart
%Aug 24 17:05:08:770 2006 Sysname RM/3/RMLOG:
 BGP.: 10.1.1.1 State is changed from ESTABLISHED to IDLE.
*Aug 24 17:05:08:786 2006 Sysname RM/6/RMDEBUG:
 BGP_GR: Peer 10.1.1.1 Gracefully Restarting
```

// The BGP neighbor 10.1.1.1 is performing GR.

```
%Aug 24 17:05:40:851 2006 Sysname RM/3/RMLOG:
 BGP.: 10.1.1.1 State is changed from OPENCONFIRM to ESTABLISHED.
```

// The BGP peer relationship has been successfully established.

```
*Aug 24 17:05:40:867 2006 Sysname RM/6/RMDEBUG:
 BGP_GR: Sent EOR to Peer 10.1.1.1 (IPv4-UNC)
```

//The BGP GR Helper finished sending initial routes and then sent an EOR message to peer 10.1.1.1.

```
*Aug 24 17:05:41:96 2006 Sysname RM/6/RMDEBUG:
 BGP_GR: Received EOR from Peer 10.1.1.1 (IPv4-UNC)
```

// The BGP GR Helper received an EOR message from peer 10.1.1.1.

debugging bgp

Syntax **debugging bgp** [*ipv4-address* | *ipv6-address*] { **keepalive** | **open** | **packet** | **raw-packet** | **route-refresh** } [**receive** | **send**] [**verbose**] }

undo debugging bgp [*ipv4-address* | *ipv6-address*] { **keepalive** | **open** | **packet** | **raw-packet** | **route-refresh** } [**receive** | **send**] [**verbose**] }

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

keepalive: Enables BGP Keepalive message debugging.

open: Enables BGP OPEN message debugging.

packet: Specifies to enable BGP packet debugging

raw-packet: Enables BGP raw packet debugging.

route-refresh: Enables BGP Route-Refresh message debugging.

receive: Enables the debugging for received BGP packets.

send: Enables the debugging for sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp** command to enable debugging for specific BGP message types.

Use the **undo debugging bgp** command to disable debugging for specific BGP message types.

Enabling debugging may affect system performance; therefore, use the command only when necessary and disable debugging once the debugging operation is complete.

By default, this debugging is disabled.

Table 226 Description on the fields of the debugging bgp command

Field	Description
Recv	Received packets
Send	Sent packets
Length: *LengthNumber*	Packet length

Table 227 Description on the fields of the debugging bgp open command

Field	Description
Version: *X*	BGP protocol version
Local AS: *X*	Local AS number
OPT Type: 2 (Capability)	Capability negotiation
CAP Type: 1 (Multiprotocol) CAP Len: 4	Multiprotocol capability: afi: 1; safi: 1
IPv4-UNC (1/1)	Capable of route-refresh
CAP Type: 2 (RouteRefresh) CAP Len: 0	
Total CAPB Len : *X*	Total capability length
Total OPT Len : *X*	Total optional parameter length

Table 228 Description on the fields of the debugging bgp refresh command

Field	Description
AFI/ SAFI	Address family/sub-address family
WTR	(When to Refresh) Wait delay for sending refresh messages

For details about UPDATE message debugging information, refer to the following section.

Examples # Display the debugging information about all the BGP messages received and sent, including Open, Keepalive, Update, and Route-refresh, while Device A and Device B are establishing a BGP peer relationship with each other.

```
<Sysname> debugging bgp
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] undo synchronization
[Sysname-bgp] peer 11.1.1.2 group 200

*0.2683484 4945 RM/6/RMDEBUG:
         BGP.: 11.1.1.2 Send OPEN, Version: 4
         Local AS: 100, HoldTime: 180, Router ID: 192.168.74.1

         OPT Type:   2 (Capability)
         CAP Type:   1 (Multiprotocol)  CAP Len: 4
                                        IPv4-UNC (1/1)
         CAP Type:   2 (RouteRefresh)   CAP Len: 0

         Total CAPB Len    : 8
         Total OPT Len     : 10
         Total Message Len : 39
```

// Information about the sent BGP Open message

```
*0.2683500 4945 RM/6/RMDEBUG:
         BGP.: 11.1.1.2 Recv OPEN Length: 39
         Version: 4, Local AS: 200, HoldTime : 180,
         BGP ID: 192.168.74.2, TotOptLen: 10

         OPT Type:   2 (Capability)     OPT Len: 8
         CAP Type:   1 (Multiprotocol)  CAP Len: 4
```

```
                                          IPv4-UNC (1/1)
         CAP Type:   2 (RouteRefresh)   CAP Len: 0
```

// Information about the received BGP Open message

```
*0.2683500 4945 RM/6/RMDEBUG:
         BGP.: 11.1.1.2 Send KEEPALIVE
         Length 19
```

// Information about the sent BGP Keepalive message

```
*0.2683609 4945 RM/6/RMDEBUG:
         BGP.: 11.1.1.2 Recv KEEPALIVE
         Length: 19
```

// Information about the received BGP Keepalive message

```
[Sysname-bgp] import-route static
*0.2710031 4945 RM/6/RMDEBUG:
         BGP.: Send UPDATE to 11.1.1.2 for following destinations :
         Origin       : Incomplete
         AS Path      : 100
         Next Hop     : 11.1.1.1
         MED          : 0
         111.1.1.1/32,
```

// Information about the sent BGP update of a redistributed static route

```
*0.2728250 4945 RM/6/RMDEBUG:
         BGP.: Recv UPDATE from 11.1.1.2 with following destinations :
         Update message length : 53
         MED          : 0
         Origin       : Incomplete
         AS Path      : 200
         Next Hop     : 11.1.1.2
         222.1.1.1/32
```

// Information about the received BGP Update of a redistributed static route

Device A and Device B has established a peer relationship. On Device A, enable debugging for the received BGP route-refresh messages. On Device B, enable debugging for the sent BGP route-refresh messages and execute the **refresh bgp all import** command.

```
<Sysname> debugging bgp route-refresh send
<Sysname> refresh bgp all import
*0.340484 Sysname RM/6/RMDEBUG:
 BGP.: 3.3.3.3 Send ROUTEREFRESH MSG :
 Length: 23, AFI: 1, SAFI: 1.
```

// Device B sent a BGP Route-refresh message, with a length of 23, address family of 1, and sub-address family of 1.

```
<Sysname> debugging bgp route-refresh receive
*0.45337687 Sysname RM/6/RMDEBUG:
 BGP.: 2.2.2.2 Recv ROUTEREFRESH MSG:
 Length: 23, AFI: 1, SAFI: 1, WTR: 0.
```

// Device A received the BGP Route-refresh message, with a length of 23, address family of 1, sub-address family of 1, and *When to Refresh* of 0.

debugging bgp timer

Syntax **debugging bgp** [*ipv4-address* | *ipv6-address*] **timer**

undo debugging bgp [*ipv4-address* | *ipv6-address*] **timer**

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **debugging bgp timer** command to enable BGP timer debugging.

Use the **undo debugging bgp timer** command to disable BGP timer debugging.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use the command only when necessary and disable debugging once the debugging operation is complete.

Table 229 Description on the fields of the debugging bgp timer command

Field	Description
CR Timer	Connection retry timer
HOLD Timer	Hold timer

Examples # Configure BGP on Device A and specify BGP peer 2.2.2.2 (Device B). On Device B which is connected to Device A, create no corresponding BGP peer. Enable BGP timer debugging on Device A.

```
<Sysname> debugging bgp timer
*0.92311078 Sysname RM/6/RMDEBUG:
 BGP_TIMER: CR Timer Expired for Peer 2.2.2.2
```

// The ConnectRetry timer for BGP peer 2.2.2.2 expired.

Configure BGP and specify a peer on Device B. The two devices establish a BGP peer relationship. Disable Device A from sending Keepalive messages to Device B. Then enable BGP timer debugging on Device B.

```
<Sysname> debugging bgp timer
*0.92311078 Sysname RM/6/RMDEBUG:
 BGP_TIMER: HOLD Timer Expired for Peer 2.2.2.2
```

// The hold timer expired on BGP peer 2.2.2.2.

debugging bgp update

Syntax **debugging bgp update** [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **acl** *acl-number:* Specifies an access control list (ACL) for filtering packet debugging information. The *acl-number* argument ranges from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies an IP prefix list for filtering the packet debugging information. *ip-prefix-name* is a string of 1 to 19 characters.

receive: Enables the debugging for received BGP packets.

send: Enables the debugging for sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update** command to enable debugging for BGP Update messages.

Use the **undo debugging bgp update** command to disable debugging for BGP Update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Table 230 Description on the fields of the debugging bgp update command

Field	Description
BGP.xxx	BGP instance name
Err/SubEr	Error code/error subcode
Errdata:	Error data
x.x.x.x/xx	Destination address/mask
RPM policy failed for policy :	Failed to pass policy xx
name:xx :	
INBOUND	Inbound policy
tnl id	Tunnel ID

Table 230 Description on the fields of the debugging bgp update command

Field	Description
afi = 196(l2vpn) safi = 128(l2vpn)	Address family is 196. Sub-address family is 128 (L2VPN).
afi = 155(vpls) safi = 128(vpls)	Address family is 155. Sub-address family is 128 (VPLS).

Examples For details, refer to the Update message debugging information for specific parameters.

debugging bgp update ipv4

Syntax **debugging bgp update ipv4** [**peer** { *ipv4-address* | *ipv4-group-name* } | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update ipv4 [**peer** { *ipv4-address* | *ipv4-group-name* } | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv4-address* | *ipv4-group-name* }: Enables/disables BGP IPv4 update debugging for the specified IPv4 peer/peer group.

ip-prefix *ip-prefix-name*: Filters the output message debugging information with the specified IP prefix list.

receive: Enables/disables debugging for received BGP updates.

send: Enables/disables debugging for sent BGP updates.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update ipv4** command to enable debugging for BGP Update messages.

Use the **undo debugging bgp update ipv4** command to disable debugging for BGP Update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Examples # Device A and Device B have established an IPv4 peer relationship. Enable debugging for BGP Update messages.

```
<Sysname> debugging bgp update ipv4
*Sep  4 16:08:20:458 2006 Sysname RM/6/RMDEBUG:
```

```
        BGP.: Send UPDATE to 11.1.1.2 for following destinations :
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.1
        Local Pref   : 100
        MED          : 0
        1.1.1.1/32,

*Sep  4 16:08:20:473 2006 Sysname RM/6/RMDEBUG:
        BGP.: Send UPDATE to 11.1.1.2 for following destinations :
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.1
        Local Pref   : 100
        MED          : 0
        11.1.1.0/24,

*Sep  4 16:08:20:473 2006 Sysname RM/6/RMDEBUG:
        BGP.: Send UPDATE to 11.1.1.2 for following destinations :
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.1
        Local Pref   : 100
        MED          : 0
        11.1.1.2/32,

*Sep  4 16:08:37:272 2006 Sysname RM/6/RMDEBUG:
        BGP.: Recv UPDATE from 11.1.1.2 with following destinations :
        Update message length : 56
        Local Pref   : 100
        MED          : 0
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.2
        2.2.2.2/32,

*Sep  4 16:08:37:304 2006 Sysname RM/6/RMDEBUG:
        BGP.: Recv UPDATE from 11.1.1.2 with following destinations :
        Update message length : 55
        Local Pref   : 100
        MED          : 0
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.2
        11.1.1.0/24,

*Sep  4 16:08:37:304 2006 Sysname RM/6/RMDEBUG:
        BGP.: Recv UPDATE from 11.1.1.2 with following destinations :
        Update message length : 56
        Local Pref   : 100
        MED          : 0
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 11.1.1.2
        11.1.1.1/32,
```

// Update messages of IPv4 address family

debugging bgp update ipv6

Syntax **debugging bgp update ipv6** [**peer** { *ipv6-address* | *ipv6-group-name* } | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update ipv6 [**peer** { *ipv6-address* | *ipv6-group-name* } | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv6-address* | *ipv6-group-name* }: Enables/disables BGP IPv6 update debugging for the specified IPv6 peer/peer group.

ip-prefix *ip-prefix-name*: Filters the output message debugging information with the specified IP prefix list.

receive: Enables/disables debugging for received BGP packets.

send: Enables/disables debugging for sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update ipv6** command to enable debugging for IPv6 BGP Update messages.

Use the **undo debugging bgp update ipv6** command to disable debugging for IPv6 BGP update messages.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

By default, this debugging is disabled.

Examples # Device A and Device B have established an IPv6 BGP peer relationship. Enable debugging for IPv6 BGP update messages.

```
<Sysname> debugging bgp update ipv6

%Sep  4 16:17:20:642 2006 Sysname RM/3/RMLOG:
 BGP.: 100::2 State is changed from OPENCONFIRM to ESTABLISHED.

*Sep  4 16:17:20:642 2006 Sysname RM/6/RMDEBUG:
         BGP.: Send UPDATE to 100::2 for following destinations :
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 100::1
         Local Pref   : 100
         MED          : 0
         11::11/128,

*Sep  4 16:17:20:642 2006 Sysname RM/6/RMDEBUG:
         BGP.: Send UPDATE to 100::2 for following destinations :
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 100::1
         Local Pref   : 100
         MED          : 0
         100::/64,

*Sep  4 16:17:20:708 2006 Sysname RM/6/RMDEBUG:
         BGP_IPV6.: Recv UPDATE from peer 100::2 with following destinations :

         Update message length : 86
         Local Pref   : 100
```

```
        MED          : 0
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 100::2
        22::22/128,

*Sep  4 16:17:20:708 2006 Sysname RM/6/RMDEBUG:
        BGP_IPV6.: Recv UPDATE from peer 100::2 with following destinations :

        Update message length : 78
        Local Pref   : 100
        MED          : 0
        Origin       : Incomplete
        AS Path      :
        Next Hop     : 100::2
        100::/64,
```

// Update messages of IPv6 address family

debugging bgp update l2vpn

Syntax **debugging bgp update l2vpn** [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

undo debugging bgp update l2vpn [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv4-address* | *group-name* }: Enables/disables BGP L2VPN Update message debugging for the specified peer/peer group.

receive: Enables/disables the debugging for received BGP packets.

send: Enables/disables the debugging for sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update l2vpn** command to enable debugging for BGP L2VPN Update messages.

Use the **undo debugging bgp update l2vpn** command to disable debugging for BGP L2VPN Update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Table 231 Description on the fields of the debugging bgp update l2vpn command

Field	Description
afi = 196(l2vpn) safi = 128(l2vpn)	Address family is 196. Sub-address family is 128(L2VPN).

Examples # In an L2VPN environment, Device A and Device B have established a BGP peer relationship. Enable debugging for BGP Update messages.

```
<Sysname> debugging bgp update l2vpn
*0.84372 Sysname RM/7/RMDEBUG:
         BGP.L2VPN: Send UPDATE to 1.1.1.1 for following destinations :
         Origin       : IGP
         AS Path      : 200
         Next Hop     : 5.5.5.5
         afi = 196(l2vpn) safi = 128(l2vpn)
         Route Distinguisher:100:1
         CE-ID:1
         label offset:0
         label base:20480


*0.92566 Sysname RM/7/RMDEBUG:
         BGP.L2VPN: Recv UPDATE from 1.1.1.1 with following destinations :
         Update message length : 88
         Origin       : IGP
         AS Path      : 100
         Next Hop     : 1.1.1.1
         afi = 196(l2vpn) safi = 128(l2vpn)
         Route Distinguisher:100:1
         CE-ID:0
         label offset:0
         label base:8192
```

// Update messages in an L2VPN environment

debugging bgp update label-route

Syntax **debugging bgp update label-route** [**peer** { *ipv4-address* | *group-name* }] [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update label-route [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv4-address* | *group-name* }: Enables/disables BGP labeled route update message debugging for the specified peer/peer group.

acl *acl-number*: Filters the output message debugging information with the specified ACL.

ip-prefix *ip-prefix-name*: Filters the output message debugging information with the specified address prefix.

receive: Enables/disables the debugging for received BGP labeled route update packets.

send: Enables/disables the debugging for sent BGP labeled route update packets.

verbose: Displays detailed debugging information.

Description

Use the **debugging bgp update label-route** command to enable debugging for BGP labeled route update messages.

Use the **undo debugging bgp update label-route** command to disable debugging for BGP labeled route update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Examples

Device A and Device B have established a BGP peer relationship and MPLS has been enabled on the connected interfaces. Enable debugging for BGP labeled route update messages.

```
<Sysname> debugging bgp update route-label
*Sep  4 16:14:32:16 2006 Sysname RM/6/RMDEBUG:
 BGP.: Send UPDATE to peer 2.2.2.2 for following destinations :

*Sep  4 16:14:32:16 2006 Sysname RM/6/RMDEBUG:
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 1.1.1.1
         Local Pref   : 100
         MED          : 0
         111.1.1.1/32 (1024)

*Sep  4 16:14:32:22 2006 Sysname RM/6/RMDEBUG:
         BGP_L3VPN.: Recv UPDATE from 2.2.2.2 with following destinations :

         Update message length : 76
         Local Pref   : 100
         MED          : 0
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 2.2.2.2
         111.2.2.2/32 (1025)
```

// Update message information of L3VPN labeled routes

```
*Sep  4 16:17:20:642 2006 Sysname RM/6/RMDEBUG:
         BGP.: Send UPDATE to 100::2 for following destinations :
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 100::1
         Local Pref   : 100
         MED          : 0
         100::/64(1025),

*Sep  4 16:17:20:708 2006 Sysname RM/6/RMDEBUG:
         BGP_IPV6.: Recv UPDATE from peer 100::2 with following destinations :

         Update message length : 86
```

```
Local Pref    : 100
MED           : 0
Origin        : Incomplete
AS Path       :
Next Hop      : 100::2
22::22/128(1027)
```

// Update message information of IPv6 labeled routes

debugging bgp update peer

Syntax **debugging bgp update peer** { *ipv4-address* | *group-name* } [**acl** *acl-number* | **ip-prefix** *ip-prefix-name*] [**receive** | **send**] [**verbose**]

undo debugging bgp update peer { *ipv4-address* | *group-name* } [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters *ipv4-address*: IPv4 peer address.

group-name: Peer group name.

acl *acl-number*: Filters the output message debugging information with the specified ACL.

ip-prefix *ip-prefix-name*: Filters the output message debugging information with the specified IP prefix list.

receive: Enables/disables the debugging for the received BGP packets.

send: Enables/disables the debugging for the sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update peer** command to enable BGP update message debugging for the specified peer/peer group.

Use the **undo debugging bgp update peer** command to disable BGP Update message debugging for the specified peer/peer group.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Examples For Update message debugging information in different networking environments, see the related commands.

debugging bgp update vpls

Syntax **debugging bgp update vpls** [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

undo debugging bgp update vpls [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv4-address* | *group-name* }: Enables/disables BGP VPLS update message debugging for the specified peer/peer group.

receive: Enables/disables the debugging for the received BGP packets.

send: Enables/disables the debugging for the sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update vpls** command to enable debugging for BGP VPLS Update messages.

Use the **undo debugging bgp update vpls** command to disable debugging for BGP VPLS Update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Table 232 Description on the fields of the debugging bgp update vpls command

Field	Description
afi = 196(vpls) safi = 128(vpls)	Address family is 196. Sub-address family is 128 (VPLS).

Examples # In a VPLS environment, Device A and Device B have established a BGP peer relationship. Enable debugging for BGP VPLS update messages.

```
<Sysname> debugging bgp update vpls
*0.84372 Sysname RM/7/RMDEBUG:
         BGP.VPLS: Send UPDATE to 1.1.1.1 for following destinations :
         Origin       : IGP
         AS Path      : 200
         Next Hop     : 5.5.5.5
         afi = 155(vpls) safi = 128(vpls)
         Route Distinguisher:100:1
         CE-ID:1
         label offset:0
         label base:20480
```

// Information about the sent VPLS update message

```
*0.92566 Sysname RM/7/RMDEBUG:
         BGP.VPLS: Recv UPDATE from 1.1.1.1 with following destinations :
         Update message length : 88
         Origin       : IGP
         AS Path      : 100
         Next Hop     : 1.1.1.1
         afi = 155(vpls) safi = 128(vpls)
         Route Distinguisher:100:1
         CE-ID:0
         label offset:0
         label base:8192
```

// Information about the received VPLS update message

debugging bgp update vpn-instance

Syntax **debugging bgp update vpn-instance** *vpn-instance-name* [**ip-prefix** *ip-prefix-name* | **peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

undo debugging bgp update vpn-instance *vpn-instance-name* [**ip-prefix** *ip-prefix-name* | **peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters *vpn-instance-name*: Enables/disables the BGP update message debugging for the specified VPN instance.

ip-prefix *ip-prefix-name*: Filters the output message debugging information with the specified IP prefix list.

peer { *ipv4-address* | *group-name* }: Enables/disables BGP update message debugging for the specified peer/peer group.

receive: Enables/disables the debugging for received BGP packets.

send: Enables/disables the debugging for the sent BGP packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update vpn-instance** command to enable update message debugging for a BGP VPN instance.

Use the **undo debugging bgp update instance** command to disable update message debugging for a BGP VPN instance.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Refer to "debugging bgp update vpnv4" on page 1035 for the description of the update message information.

Examples None

debugging bgp update vpnv4

Syntax **debugging bgp update vpnv4** [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

undo debugging bgp update vpnv4 [**peer** { *ipv4-address* | *group-name* }] [**receive** | **send**] [**verbose**]

View User view

Default Level 1: Monitor level

Parameters **peer** { *ipv4-address* | *group-name* }: Enables/disables BGP Update message debugging for the specified peer/peer group.

receive: Enables/disables the debugging for the received BGP VPNv4 packets.

send: Enables/disables the debugging for the sent BGP VPNv4 packets.

verbose: Displays detailed debugging information.

Description Use the **debugging bgp update vpnv4** command to enable debugging for BGP VPNv4 Update messages.

Use the **undo debugging bgp update vpnv4** command to disable debugging for BGP VPNv4 Update messages.

By default, this debugging is disabled.

Enabling debugging may affect system performance; therefore, use this command only when necessary and disable debugging once the debugging operation is complete.

Examples # Device A and Device B have established a BGP peer relationship under the VPNv4 instance. On Device A, enable debugging for received BGP VPNv4 update messages; on Device B, enable debugging for sent BGP VPNv4 update messages.

```
<Sysname> debugging bgp update vpnv4

%Sep  4 16:14:32:00 2006 Sysname RM/3/RMLOG:
 BGP.: 2.2.2.2 State is changed from OPENCONFIRM to ESTABLISHED.

*Sep  4 16:14:32:16 2006 Sysname RM/6/RMDEBUG:
 BGP_L3VPN.: Send UPDATE to peer 2.2.2.2 for following destinations :

*Sep  4 16:14:32:16 2006 Sysname RM/6/RMDEBUG:
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 1.1.1.1
```

```
         Local Pref   : 100
         MED          : 0
         Ext-Community: <1 : 1>
         111.1.1.1/32 (RD 100:1,Label 1024),

*Sep  4 16:14:32:22 2006 Sysname RM/6/RMDEBUG:
         BGP_L3VPN.: Recv UPDATE from 2.2.2.2 with following destinations :

         Update message length : 92
         Local Pref   : 100
         MED          : 0
         Ext-Community: <1 : 1>
         Origin       : Incomplete
         AS Path      :
         Next Hop     : 2.2.2.2
         111.2.2.2/32 (RD 100:2,Label 1024),

*Sep  4 16:14:33:164 2006 Sysname RM/6/RMDEBUG:
 BGP_L3VPN: L3VPN Process IP Address 111.2.2.2 src instance VPNV4 dest instance
red
 LocRemCross:No Import Policy .Route Added To Target Instance
```

// Update message information of VPNv4

74 IS-IS CONFIGURATION COMMANDS

area-authentication-mode

Syntax **area-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]

undo area-authentication-mode

View IS-IS view

Parameters **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password encrypted with MD5.

password: Password to be set. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plaintext password can be a string of up to 16 characters, such as **user918**. A cipher password must be a ciphertext string of up to 24 characters, such as **(TT8F]Y5SQ=^Q'MAF4<1!!**.

ip: Specifies the system to check the configuration for the corresponding field of IP in LSP.

osi: Specifies the system to check the configuration for the corresponding field of OSI in LSP.

*Whether a password should use **ip** or **osi** is not affected by the actual network environment.*

Description Use the **area-authentication-mode** command to configure the area authentication mode to insert the area authentication password into all the sent level-1 packets (LSP, CSNP, and PSNP) in the predefined way and verify the authentication password of the received level-1 pockets.

Use the **undo area-authentication-mode** command to restore the default.

By default, no area authentication mode is configured in the system; that is, the system authenticates no level-1 packets received and is configured with no password.

Configuring an area authentication mode can prevent the routing information learned by any untrusted routers from being added to the local LSDB.

Related commands: **reset isis all**, **domain-authentication-mode**, **isis authentication-mode**

Examples # Set the area authentication password to hello, and the authentication mode to simple.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] area-authentication-mode simple hello
```

auto cost enable

Syntax **auto-cost enable**

undo auto-cost enable

View IS-IS view

Parameters None

Description Use the **auto-cost enable** command to enable interfaces of the current IS-IS process to calculate interface cost automatically.

Use the **undo auto-cost enable** command to disable the function.

This function is disabled by default.

The preference of interface cost set by the **auto-cost** command is lower than that set by the **circuit-cost** command. The preference from high to low is: the cost set by the **isis cost** command, the global cost set by the **circuit cost** command, the cost automatically calculated and the default cost.

When the **cost-style** is **wide** or **wide-compatible**, the cost value of an interface is calculated by using the following formula:

cost = (reference value/bandwidth)×10.

Related commands: **bandwidth-reference (IS-IS view)**, **cost-style**.

Examples # Enable interfaces of IS-IS process 1 to calculate interface cost automatically.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] auto-cost enable
```

bandwidth-reference (IS-IS view)

Syntax **bandwidth-reference** *value*

undo bandwidth-reference

View IS-IS view

Parameters **value**: Bandwidth reference value in Mbps, ranging from 1 to 2147483648.

Description Use the **bandwidth-reference** command to set the bandwidth reference value for calculating link cost.

Use the **undo bandwidth-reference** command to restore the default.

By default, the reference value is 100 Mbps.

In the case no interface cost is specified in interface view or system view and automatic cost calculation is enabled:

- When the cost style is **wide** or **wide-compatible**, IS-IS automatically calculates the interface cost based on the interface bandwidth, using the formula: interface cost = bandwidth reference value/interface bandwidth, and the maximum calculated cost is 16777214.
- When the cost style is **narrow**, **narrow-compatible**, or **compatible**, if the interface is a loopback interface, the cost value is 0; otherwise, the cost value is automatically calculated as follows: if the interface bandwidth is in the range of 1 M to 10 M, the interface cost is 60; if the interface bandwidth is in the range of 11 M to 100 M, the interface cost is 50; if the interface bandwidth is in the range of 101 M to 155 M, the interface cost is 40; if the interface bandwidth is in the range of 156 M to 622 M, the interface cost is 30; if the interface bandwidth is in the range of 623 M to 2500 M, the interface cost is 20, and the default interface cost of 10 is used for any other bandwidths.

Related commands: **auto cost enable**.

Examples # Configure the bandwidth reference of IS-IS process 1 as 200 Mbps.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] bandwidth-reference 200
```

circuit-cost

Syntax **circuit-cost** *value* [**level-1** | **level-2**]

undo circuit-cost [**level-1** | **level-2**]

View IS-IS view

Parameters *value*: Specifies the global link cost value. The value range varies with cost types.

- For types **narrow, narrow-compatible** and **compatible**: The cost value ranges from 0 to 63.
- For types **wide** and **wide-compatible**: The cost value ranges from 0 to 16777215.

level-1: Applies the link cost to Level-1.

level-2: Applies the link cost to Level-2.

Description Use the **circuit-cost** command to set a global link cost.

Use the **undo circuit-cost** command to restore the default.

By default, the global link cost is not configured.

If no keyword is specified, the specified cost applies to Level-1-2.

The preference of interface cost from high to low is: the cost set by the **isis cost** command, the global cost set by the **circuit-cost** command, the cost automatically calculated (**auto-cost)** and the default cost.

Related commands: **isis cost**, **cost-style**.

Examples # Set the global Level-1 link cost of IS-IS process 1 to 11.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] circuit-cost 11 level-1
```

cost-style

Syntax **cost-style** { **narrow** | **wide** | **wide-compatible** | { **compatible** | **narrow-compatible** } [**relax-spf-limit**] }

undo cost-style

View IS-IS view

Parameters **narrow**: Specifies to receive and send only packets of narrow cost style (The narrow cost ranges from 0 to 63).

wide: Specifies to receive and send only packets of wide cost style (The wide cost ranges from 0 to 16777215).

compatible: Specifies to receive and send both wide and narrow style packets.

narrow-compatible: Specifies to receive both narrow and wide style packets, but send only narrow style packets.

wide-compatible: Specifies to receive both narrow and wide style packets, but send only wide style packets.

relax-spf-limit: Specifies to allow receiving routes with cost bigger than 1023. If this keyword is not configured, any route with cost bigger than 1023 will be discarded. This keyword is only available when keywords **compatible** and **narrow-compatible** are included.

Description Use the **cost-style** command to set the cost style of packets.

Use the **undo cost-style** command to restore the default.

Only packets of narrow cost style can be received and sent by default.

Related commands: **isis cost**.

Examples # Configure the router to send only packets of narrow cost style, but receive both narrow and wide cost style ones.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] cost-style narrow-compatible
```

default-route-advertise (IS-IS view)

Syntax **default-route-advertise** [**route-policy** *route-policy-name* | [**level-1** | **level-2** | **level-1-2**]] *

undo default-route-advertise [**route-policy** *route-policy-name*]

View IS-IS view

Parameters *route-policy-name*: Specifies the name of a routing policy, a string of 1 to 19 characters.

level-1: Specifies the level of the default route as Level-1.

level-2: Specifies the level of the default route as Level-2.

level-1-2: Specifies the level of the default route as Level-1-2.

If no level is specified, a Level-2 default route is generated.

Description Use the **default-route-advertise** command to generate a Level-1 or Level-2 default route.

Use the **undo default-route-advertise** command to disable the function.

This function is disabled by default.

The Level-1 default route is advertised to other routers in the same area, while the Level-2 default route is advertised to all the Level-2 and Level-1-2 routers.

Using the **apply isis level-1** command in routing policy view will generate a default route in L1 LSP. Using the **apply isis level-2** command in routing policy view will generate a default route in L2 LSP. Using the **apply isis level-1-2** command in routing policy view will generate a default route in L1 LSP and L2 LSP respectively.

Examples # Generate a default route in L2 LSP.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] default-route-advertise
```

display isis brief

Syntax **display isis brief** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: IS-IS process ID, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a string of 1 to 31 characters.

Description Use the **display isis brief** command to view brief IS-IS configuration information.

Examples # Display brief IS-IS configuration information.

```
<Sysname> display isis brief

                  ISIS 1 Protocol Brief Information :


network-entity:
    10.0000.0000.0001.00
is-level :level-1-2
cost-style:  narrow
preference :  15
Lsp-length receive :  1497
Lsp-length originate :  level-1 1497
                        level-2 1497
Timers:
    spf-slice-size:  0
    lsp-max-age:  1200
    lsp-refresh:  900
    Interval between SPFs:  10
```

Table 233 Description on the fields of the display isis brief command

Field	Description
network-entity	Network entity name
is-level	IS-IS Routing level
cost-style	Cost style
preference	Preference
Lsp-length receive	Maximum LSP that can be received
Lsp-length originate	Maximum LSP that can be generated
Timers	Timers
spf-slice-size	Time of each SPF calculation slice (0 means SPF calculation time is not split.)
lsp-max-age	Maximum life period of LSP

Table 233 Description on the fields of the display isis brief command

Field	Description
lsp-refresh	Refresh period of LSP
Interval between SPFs	Interval between SPF calculations

display isis debug-switches

Syntax **display isis debug-switches** { *process-id* | **vpn-instance** *vpn-instance-name* }

View Any view

Parameters *process-id*: Specifies the ID of an IS-IS process, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **display isis debug-switches** command to display the current IS-IS debugging state.

Examples # Display the debugging state of IS-IS process 1.

```
<Sysname> display isis debug-switches 1
IS-IS - Debug settings.
        IS-IS SPF Triggering Events debugging is on
```

display isis graceful-restart status

Syntax **display isis graceful-restart status** [**level-1** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **level-1**: Displays the IS-IS Level-1 Graceful Restart state.

level-2: Displays the IS-IS Level-2 Graceful Restart state.

process-id: IS-IS Process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 characters.

Description Use the **display isis graceful-restart status** command to display IS-IS Graceful Restart status.

Examples # Display IS-IS Graceful Restart status.

```
<Sysname> display isis graceful-restart status
                Restart information for IS-IS(1)
--------------------------------------------------------------------
IS-IS(1) Level-1 Restart Status
```

```
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  Number of LSPs Awaited: 3
  T3 Timer Status:
    Remaining Time: 239
  T2 Timer Status:
    Remaining Time: 59

IS-IS(1) Level-2 Restart Status
Restart Interval: 150
SA Bit Supported
  Total Number of Interfaces = 1
  Restart Status: RESTARTING
  Number of LSPs Awaited: 3
  T3 Timer Status:
    Remaining Time: 239
  T2 Timer Status:
Remaining Time: 59
```

Table 234 Description on the fields of the display isis graceful-restart status command

Field	Description
Restart Interval	Graceful Restart interval
SA Bit Supported	The SA bit is set
Total Number of Interfaces = 1	The current IS-IS interface number
Restart Status:	Graceful Restart status
T3 Timer Status	Remaining time of T3 timer
T2 Timer Status:	Remaining time of T2 Timer

display isis interface

Syntax **display isis interface** [[**traffic-eng** | **verbose**] * | **tunnel**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **traffic-eng**: Displays IS-IS traffic engineering information.

verbose: Displays IS-IS interface detail information.

tunnel: Displays IS-IS tunnel information.

process-id: IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: VPN instance name, a string of 1 to 31 characters.

Description Use the **display isis interface** command to view IS-IS enabled interface information.

The information displayed by this command includes interface name, interface IP address, interface link state and so on. Besides all the information displayed by

display isis interface, using the **display isis interface verbose** command displays other interface related information, such as CSNP packets broadcast intervals, Hello packets broadcast intervals and the number of invalid Hello packets.

Examples # Display IS-IS enabled interface information.

```
<Sysname> display isis interface
                       Interface information for ISIS(1)
                       --------------------------------
Interface: Ethernet1/0
Id      IPV4.State        IPV6.State     MTU    Type    DIS
001       Up                Down       1497    L1/L2   No/No
```

Display detailed IS-IS interface information.

```
<Sysname> display isis interface verbose
                       Interface information for ISIS(1)
                       --------------------------------
Interface: Ethernet1/0
Id     IPV4.State             IPV6.State        MTU    Type    DIS
001        Up                      Down         1497   L1/L2   No/No
  SNPA Address               : 0000-5e19-6d00
  IP Address                 : 192.168.0.1
  Secondary IP Address(es)   :
  IPV6 Link Local Address    :
  IPV6 Global Address(es)    :
  Csnp Timer Value           :  L1    10  L2    10
  Hello Timer Value          :  L1    40  L2    10
  Hello Multiplier Value     :  L1     3  L2    30
  Lsp Timer Value            :  L12    1
  Cost                       :  L1    10  L2    10
  Priority                   :  L1    64  L2    64
  Retransmit Timer Value     :  L12    5
  BFD                        :  Disabled
```

Table 235 Description on the fields of the display isis interface command

Field	Description
Interface	Interface
Id	Circuit ID
IPV4.State	IPv4 state
IPV6.State	IPv6 state
MTU	Interface MTU
Type	Interface link type
DIS	Designated IS
SNPA Address	Subnet access point address
IP Address	Primary IP address
Secondary IP Address(es)	Secondary IP addresses
IPV6 Link Local Address	IPv6 link local address
IPV6 Global Address(es)	IPv6 global address
Csnp Timer Value	Interval for sending CSNP packets
Hello Timer Value	Interval for sending Hello packets

Table 235 Description on the fields of the display isis interface command

Field	Description
Hello Multiplier Value	Number of invalid Hello packets
Lsp Timer Value	Interval for sending LSP packets
Cost	Cost
Priority	Preference
Retransmit Timer Value	LSP retransmission interval over point-to-point link
BFD	Whether BFD is enabled

display isis license

Syntax **display isis license**

View Any view

Parameters None

Description Use the **display isis license** command to display the information of the IS-IS license.

Examples # Display the information of the IS-IS license.

```
[Sysname] display isis license

                     ISIS Shell License Values
                     _________________________

 Feature Name         Active     Controllable
 ISIS Protocol        YES        NO
 IPV6                 YES        NO
 RESTART              YES        NO
 TE                   YES        NO
 MI                   YES        NO

 Resource Name             MinVal     MaxVal     CurrVal    Controllable
 Max Processes Resource    1          1024       500        0
 Max Paths Resource        1          6          3          0
 Max IPv4 Rt Resource      400000     400000     400000     0
 Max IPv6 Rt Resource      400000     400000     400000     0

                     ISIS Core License Values
                     ________________________

 Feature Name         Active
 ISIS Protocol        YES
 IPV6                 YES
 RESTART              YES
 TE                   YES
 MI                   YES

 Resource Name             Current Value
 Max Processes Resource    500
 Max Paths Resource        3
 Max IPv4 Rt Resource      400000
 Max IPv6 Rt Resource      400000
```

Table 236 Description on the fields of the display isis license command

Field	Description
ISIS Shell License Values	License values of ISIS shell
Feature Name	Feature name
Active	Whether the state is active.
Controllable	Whether support reading configuration through License file.
ISIS Protocol	IS-IS Protocol
IPV6	Whether IPv6 is active or not.
RESTART	Graceful Restart (GR)
TE	Traffic Engineering
MI	Multi-instance
Resource Name	Resource name
MinVal	Minimum value
MaxVal	Maximum value
CurrVal	Current value
ISIS Core License Values	License values of ISIS Core
Max Processes Resource	Maximum number of processes supported
Max Paths Resource	Maximum equal cost paths
Max IPv4 Rt Resource	Maximum IPv4 routes supported
Max IPv6 Rt Resource	Maximum IPv6 routes supported

The license information varies with device models.

display isis lsdb

Syntax **display isis lsdb** [[**l1** | **l2** | **level-1** | **level-2**] | [**lsp-id** *LSPID* | **lsp-name** *lspname*] | **local** | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **l1**, **level-1**: Specifies level-1 LSDB.

l2, **level-2**: Specifies level-2 LSDB.

LSPID: LSP ID, in the form of sysid. Pseudo ID-fragment num.

lspname: LSP name, in the form of Symbolic name.[Pseudo ID]-fragment num.

local: Displays LSP information generated locally.

verbose: Displays LSDB detailed information.

process-id: IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters.

If no level is specified, then both Level-1 and Level-2 (or Level-1-2) link state databases are displayed by default.

Description Use the **display isis lsdb** command to display IS-IS link state database.

Examples # Display Level-1 LSDB information.

```
<Sysname> dis isis lsdb level-1

                        Database information for ISIS(1)
                        --------------------------------

                          Level-1 Link State Database

LSPID                     Seq Num      Checksum      Holdtime      Length  ATT/P/OL
-------------------------------------------------------------------------------
bbbb.cccc.dddd.00-00* 0x0000001d 0x165        820           36     1/0/0

    *-Self LSP, +-Self LSP(Extended), ATT-Attached, P-Partition, OL-Overload
```

Table 237 Description on the fields of the display isis lsdb command

Field	Description
LSPID	Link state packet ID
Seq Num	LSP sequence number
Checksum	LSP checksum
Holdtime	LSP holdtime
Length	LSP length
ATT/P/OL	Attach bit (ATT)
	Partition bit (P)
	Overload bit (OL)

display isis mesh-group

Syntax **display isis mesh-group** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: Specifies an IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, in the range of 1 to 31 characters.

Description Use the **display isis mesh-group** command to display IS-IS mesh-group.

Examples # Add the Serial2/0 interface and Serial2/1 interface on a router to mesh-group 100.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis mesh-group 100
[Sysname-Serial2/0] quit
[Sysname] interface serial 2/1
[Sysname-Serial2/1] isis mesh-group 100
```

Display the configuration information of IS-IS mesh-group.

```
[Sysname-Serial2/1] display isis mesh-group
              Mesh Group information for ISIS(1)
-------------------------------------------------------------------------
Interface          Status
Serial2/0         100
Serial2/1         100
```

display isis name-table

Syntax **display isis name-table** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: VPN instance name, in the range of 1 to 31 characters.

Description Use the **display isis name-table** command to display the host name-to-system ID mapping table.

Examples # Configure a name for the local IS-IS system.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

Configure a static mapping for the remote IS-IS system (0000.0000.0041).

```
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

Display the IS-IS host name-to-system ID mapping table.

```
[Sysname-isis-1] display isis name-table
              Name table information for ISIS(1)
-------------------------------------------------------------
System ID            Hostname                          Type
6789.0000.0001       RUTA                              DYNAMIC
0000.0000.0041       RUTB                              STATIC
```

Table 238 Description on the fields of the display isis name-table command

Field	Description
System ID	System ID
Hostname	Hostname name of the system ID
Type	Mapping type of system ID to host name (static or dynamic)

display isis peer

Syntax **display isis peer** [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **verbose**: When this parameter is used, the area address advertised in a neighbor's Hello packet will be displayed. Otherwise the system displays only the summary information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, in the range of 1 to 31 characters.

Description Use the **display isis peer** command to display IS-IS neighbor information.

Besides all the information displayed using the **display isis peer** command, the **display isis peer verbose** command displays neighbor area address, hold time of Up state and direct interface's IP address.

Examples # Display detailed IS-IS neighbor information.

```
<Sysname> display isis peer verbose
                          Peer information for ISIS(1)
                          ----------------------------
System Id: 0000.0000.0003
Interface: Ethernet1/0           Circuit Id: 0000.0000.0003.01
State: Up  HoldTime: 8s          Type: L1(L1L2)        PRI: 64
Area Address(es):10
Peer IP Address(es): 192.168.0.3
Uptime: 00:14:03
Adj Protocol:  IPV4
```

Table 239 Description on the fields of the display isis peer command

Field	Description
System Id	System ID
Interface	Interface connecting to the neighbor
Circuit Id	Circuit ID
State	State
HoldTime	Holdtime
Type	Type of the neighbor
PRI	DIS Priority
Area Address(es)	The neighbor's area address
Peer IP Address(es)	Interface IP address of the neighbor
Uptime	Time being up
Adj Protocol	Adjacency protocol

display isis route

Syntax **display isis route** [**ipv4**] [[**level-1** | **level-2**] | **verbose**] * [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **ipv4**: Displays IS-IS IPv4 routing information (the default).

verbose: Displays IS-IS detailed IPv4 routing information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, in the range of 1 to 31 characters.

level-1: Displays Level-1 IS-IS routes.

level-2: Displays Level-2 IS-IS routes.

If no level is specified, then both Level-1 and Level-2 (Level-1-2) routing information will be displayed.

Description Use the **display isis route** command to display IS-IS IPv4 routing information.

Examples # Display IS-IS IPv4 routing information

```
<Sysname> display isis route
                        Route information for ISIS(1)
                        -----------------------------

                     ISIS(1) IPv4 Level-1 Forwarding Table
                     -------------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
------------------------------
 12.12.12.0/24        10         NULL    Eth0/1/0        Direct          D/L/-
 24.24.24.0/24        20         NULL    Eth0/1/0        12.12.12.2      R/L/-
 2.2.2.2/32           10         NULL    Eth0/1/0        12.12.12.2      R/L/-
 2.2.3.2/32           10         NULL    Eth0/1/0        12.12.12.2      R/L/-

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set


                     ISIS(1) IPv4 Level-2 Forwarding Table
                     -------------------------------------

 IPV4 Destination     IntCost    ExtCost ExitInterface   NextHop         Flags
--------------------------------------------------------------------------------
------------------------------
 12.12.12.0/24        10         NULL    Eth0/1/0        Direct          D/L/-
 24.24.24.0/24       20        NULL
 2.2.2.2/32          10        NULL
 2.2.3.2/32          10        NULL

      Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 240 Description on the fields of the display isis route command

Field	Description
IPV4 Destination	IPv4 destination address
IntCost	Interior routing cost
ExtCost	Exterior routing cost
ExitInterface	Exit interface
NextHop	Next hop

Table 240 Description on the fields of the display isis route command

Field	Description
Flags	Routing state flag
	D: Direct route.
	R: The route has been added into the routing table.
	L: The route has been broadcast.
	U: A route's penetration flag. Setting it to UP can prevent an LSP sent from L2 to L1 from being sent back to L2.

display isis spf-log

Syntax **display isis spf-log** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: Specifies an IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **display isis spf-log** command to display IS-IS SPF log record.

Examples # Display IS-IS SPF log record.

```
<Sysname> display isis spf-log
                       SPF Log information for ISIS(1)
                       -------------------------------
   Level    Trig.Event                      No.Nodes  Duration   StartTime
   L2       IS_SPFTRIG_PERIODIC             2         0          13:3:24
   L1       IS_SPFTRIG_PERIODIC             2         0          13:18:8
   L2       IS_SPFTRIG_PERIODIC             2         0          13:18:8
   L1       IS_SPFTRIG_PERIODIC             2         0          13:32:28
   L2       IS_SPFTRIG_PERIODIC             2         0          13:32:28
   L1       IS_SPFTRIG_PERIODIC             2         0          13:44:0
   L2       IS_SPFTRIG_PERIODIC             2         0          13:44:0
   L1       IS_SPFTRIG_PERIODIC             2         0          13:55:43
-->L2       IS_SPFTRIG_PERIODIC             2         0          13:55:43
   L1       IS_SPFTRIG_PERIODIC             2         0          11:54:12
   L2       IS_SPFTRIG_PERIODIC             2         0          11:54:12
   L1       IS_SPFTRIG_PERIODIC             2         0          12:7:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:7:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:21:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:21:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:35:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:35:24
   L1       IS_SPFTRIG_PERIODIC             2         0          12:49:24
   L2       IS_SPFTRIG_PERIODIC             2         0          12:49:24
   L1       IS_SPFTRIG_PERIODIC             2         0          13:3:24
```

Table 241 Description on the fields of the display isis spf-log command

Field	Description
Level	SPF calculation level
Trig.Event	SPF triggered event
No.Nodes	Number of SPF calculation nodes

Table 241 Description on the fields of the display isis spf-log command

Field	Description
Duration	SPF calculation duration
StartTime	SPF calculation start time

display isis statistics

Syntax **display isis statistics** [**level-1** | **level-2** | **level-1-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters **level-1**: IS-IS Level-1 statistic information.

level-2: IS-IS Level-2 statistic information.

level-1-2: IS-IS Level-1-2 statistic information.

process-id: Specifies an IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **display isis statistics** command to display the statistic information of IS-IS process, including the number of routes learned from other IS-IS routers, the number of routes redistributed from other protocols and the number of LSP generated locally.

Examples # Display IS-IS statistic information.

```
<Sysname> display isis statistics

                      Statistics information for ISIS(1)
                      ----------------------------------

                             Level-1 Statistics
                             ------------------

Learnt routes information:
         Total IPv4 Learnt Destinations: 4
         Total IPv6 Learnt Destinations: 0

Imported routes information:
         IPv4 Imported Routes:
                         Static: 0       Direct: 0
                         ISIS:   0       BGP:    0
                         RIP:    0       OSPF:   0
         IPv6 Imported Routes:
                         Static: 0       Direct: 0
                         ISISv6: 0       BGP4+:  0
                         RIPng:  0       OSPFv3: 0

Lsp information:
```

```
                    LSP Source ID:          No. of used LSPs
                    0000.0000.0002                  001
```

Table 242 Description on the fields of the display isis statistics command

Field		Description
Statistics information for ISIS(*processid*)		Statistics for the ISIS process
Level-1 Statistics		Level-1 Statistics
Level-2 Statistics		Level-2 Statistics
Learnt routes information		Number of learnt IPv4 routes Number of learnt IPv6 routes
Imported routes information	IPv4 Imported Routes	Redistributed IPv4 routes ■ Static ■ Direct ■ ISIS ■ BGP ■ RIP ■ OSPF
	IPv6 Imported Routes	Redistributed IPv6 routes ■ Static ■ Direct ■ ISISv6 ■ BGP4+ ■ RIPng ■ OSPFv3
Lsp information		LSP information ■ LSP Source ID: ID of the source system ■ No. of used LSPs: number of used LSPs

domain-authentication-mode

Syntax **domain-authentication-mode** { **simple** | **md5** } *password* [**ip** | **osi**]

undo domain-authentication-mode

View IS-IS view

Parameters **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password encrypted with MD5.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or cipher text. A plain text password is a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **_(TT8F]Y5SQ=^Q'MAF4<1!!**.

ip: Specifies to check the IP related fields in a LSP.

osi: Specifies to check the OSI related fields in a LSP.

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

Description Use the **domain-authentication-mode** command to configure the routing domain authentication mode to insert the area authentication password into all the sent level-2 packets (LSP, CSNP, and PSNP) in the predefined way and verify the authentication password of the received level-2 pockets.

Use the **undo domain-authentication-mode** command to cancel the routing domain authentication mode configuration.

By default, no routing domain authentication mode is configured in the system; that is, the system authenticates no level-2 packets received and is configured with no password.

Related commands: **area-authentication-mode**, **isis authentication-mode**.

Examples # Use the simple mode and password "123456" to authenticate level-2 routing packets.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] domain-authentication-mode simple 123456
```

filter-policy export (IS-IS view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **export** [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **direct** | **static**]

undo filter-policy export [**isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **bgp** | **direct** | **static**]

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter outgoing redistributed routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter outgoing redistributed routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter outgoing redistributed routes, a string of 1 to 19 characters.

isis *process-id*: Filters outgoing routes redistributed from an IS-IS process. The process ID is in the range of 1 to 65535.

ospf *process-id*: Filters outgoing routes redistributed from an OSPF process. The process ID is in the range of 1 to 65535.

rip *process-id*: Filters outgoing routes redistributed from a RIP process. The process ID is in the range of 1 to 65535.

bgp: Filters outgoing routes redistributed from BGP.

direct: Filters outgoing redistributed **direct** routes.

static: Filters outgoing redistributed **static** routes.

If no parameter is specified, the system will filter all outgoing redistributed routing information.

Description Use the **filter-policy export** command to configure IS-IS to filter outgoing redistributed routes.

Use the **undo filter-policy export** command to disable IS-IS from filtering outgoing redistributed routes.

IS-IS does not filter outgoing redistributed routes by default.

In some cases, only redistributed routing information satisfying certain conditions can be advertised. You can use the **filter-policy** command to reference filtering conditions.

Related commands: **filter-policy import (IS-IS view)**.

Examples # Reference ACL 2000 to filter outgoing redistributed routes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 export
```

filter-policy import (IS-IS view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } **import**

undo filter-policy import

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter incoming routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter incoming routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter incoming routes, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to configure IS-IS to filter incoming routing information.

Use the **undo filter-policy import** command to disable IS-IS from filtering incoming routing information.

IS-IS does not filter incoming routing information by default.

In some cases, only the routing information satisfying certain conditions can be received. You can reference filtering conditions using the **filter-policy** command.

Related commands: **filter-policy export (IS-IS view)**.

Examples # Reference ACL 2000 to filter incoming routing information.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] filter-policy 2000 import
```

flash-flood

Syntax **flash-flood** [**flood-count** *flooding-count* | **max-timer-interval** *flooding-interval* | [**level-1** | **level-2**]] *

undo flash-flood [**level-1** | **level-2**]

View IS-IS view

Parameters **flood-count** *flooding-count*: Specifies the maximum number of LSPs to be sent in the fast-flooding process, ranging from 1 to 15. The default is 5.

max-timer-interval *flooding-interval*: Specifies the delay interval (in milliseconds) between when it is enabled and when it begins, ranging from 10 to 50000. The default is 10.

level-1: Specifies to configure fast-flooding on **level-1** only.

level-2: Specifies to configure fast-flooding on **level-2** only. If no level is configured, the fast-flooding will be available on both **level-1** and **level-2** by default.

Description Use the **flash-flood** command to enable IS-IS LSP fast flooding and configure related parameters, including the maximum number of LSPs to be sent and the delay time before flooding.

Use the **undo flash-flood** command to disable fast-flooding.

Fast flooding is disabled by default.

Using this command can speed up LSP flooding that is triggered by topology changes, so as to reduce LSDB convergence time.

Examples # Enable fast flooding and configure the maximum LSPs be sent as 10 and the delay time as 100 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] flash-flood flood-count 10 max-timer-interval 100
```

graceful-restart (IS-IS view)

Syntax **graceful-restart**

undo graceful-restart

View IS-IS view

Parameters None

Description Use the **graceful-restart** command to enable the IS-IS Graceful Restart capability.

Use the **undo graceful-restart** command to disable the IS-IS Graceful Restart capability.

By default, IS-IS Graceful Restart capability is disabled.

Examples # Enable the Graceful Restart capability for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart
```

graceful-restart interval (IS-IS view)

Syntax **graceful-restart interval** *interval-value*

undo graceful-restart interval

View IS-IS view

Parameters *interval-value*: Graceful Restart interval, in the range 30 to 1800 seconds.

Description Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 300 seconds.

Examples # Configure the Graceful Restart interval for IS-IS process 1 as 120 seconds.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart interval 120
```

graceful-restart suppress-sa

Syntax **graceful-restart suppress-sa**

undo graceful-restart suppress-sa

View IS-IS view

Parameters None

Description Use the **graceful-restart suppress-sa** command to set the SA (Suppress-Advertisement) bit during restart.

Use the **undo graceful-restart suppress-sa** command to clear the SA bit during restart.

By default, the SA bit is cleared during restart.

Note that:

- A router that starts at the first time does not maintain the forwarding state. For a router that restarts IS-IS, copies of LSPs generated by this router during the previous incarnation may still exist in the lSP databases of other routers in the network.
- Copies of LSPs in the LSP databases in other routers which may look "newer" than LSPs generated by the restarting router after it initializes LSP fragment sequence numbers. This may result in temporary blackholes until subsequent LSPs with higher sequence numbers are regenerated.
- These blackholes can be avoided if the neighbors suppress advertising the previous adjacencies to the restarting router until the latter has flooded LSPs with higher sequence numbers.

Examples # Set the SA bit during Graceful Restart.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] graceful-restart suppress-sa
```

import-route (IS-IS view)

Syntax **import-route** { **isis** [*process-id*] | **ospf** [*process-id*] | **rip** [*process-id*] | **bgp** [**allow-ibgp**] | **direct** | **static** } [**cost** *cost* | **cost-type** { **external** | **internal** } | [**level-1** | **level-1-2** | **level-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo import-route { **isis** [*process-id*] | **ospf** [*process-id*] | **rip** [*process-id*] | **bgp** | **direct** | **static** }

View IS-IS view

Parameters **isis** [*process-id*]: Redistributes routes from a specified ISIS process. *process-id* is in the range of 1 to 65535.

ospf [*process-id*]: Redistributes routes from a specified OSPF process. *process-id* is in the range of 1 to 65535.

rip [*process-id*]: Redistributes routes from a specified RIP process. *process-id* is in the range of 1 to 65535.

bgp: Redistributes BGP routes.

allow-ibgp: Redistributes IBGP routes.

direct: Redistributes direct routes.

static: Redistributes static routes.

cost: Specifies a cost for redistributed routes.

The range of the cost depends on it type:

- For the types of narrow, narrow-compatible and compatible, the cost ranges from 0 to 63.
- For the types of wide, wide-compatible, the cost ranges from 0 to 16777215.

cost-type { **external** | **internal** }: Specifies a cost type. The **internal** type indicates the cost of routes within an area; the **external** type indicates the cost of routes between areas. The type is **external** by default. The keywords are valid only when the cost type is narrow, narrow-compatible or compatible.

level-1: Redistributes routes into the Level-1 routing table.

level-2: Redistributes routes into the Level-2 routing table. If no level is specified, the routes are redistributed into the Level-2 routing table by default.

level-1-2: Redistributes routes into both Level-1 and Level-2 routing tables.

route-policy *route-policy-name*: Redistributes only routes satisfying the matching conditions of a routing policy, the name of which is a string of 1 to 19 characters.

tag *tag*: Specifies a tag value for redistributed routes from 1 to 4294967295.

Description Use the **import-route** command to redistribute routes from other protocols.

Use the **undo import-route** command to disable route redistribution.

Route redistribution is not available by default.

IS-IS takes all the redistributed routes as external routes to destinations outside the IS-IS routing domain.

Related commands: **import-route isis level-2 into level-1**.

Using the import-route bgp command redistributes only EBGP routes. Using the import-route bgp allow-ibgp command redistributes also IBGP routes, but this may cause routing loops. Be cautious with this command.

Examples # Redistribute static routes and set the cost to 15.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route static cost 15
```

import-route isis level-2 into level-1

Syntax **import-route isis level-2 into level-1** [**filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*] *

undo import-route isis level-2 into level-1

View IS-IS view

Parameters *acl-number*: Specifies the number of an ACL that is used to filter redistributed routes, ranging from 2000 to 3999.

ip-prefix *ip-prefix-name*: Specifies the name of an IP prefix list that is used to filter redistributed routes, a string of 1 to 19 characters.

route-policy *route-policy-name*: Specifies the name of a routing policy that is used to filter redistributed routes, a string of 1 to 19 characters.

tag *tag*: Specifies a tag value from 1 to 4294967295 for redistributed routes.

Description Use the **import-route isis level-2 into level-1** command to redistribute routes from Level-2 to Level-1area.

Use the **undo import-route isis level-2 into level-1** command to disable this redistribution.

The redistribution is not available by default.

Note that:

- You can specify a routing policy in the **import-route isis level-2 into level-1** command to filter routes from Level-2 to Level-1. Other routing policies specified for route reception and redistribution does not affect the route leaking.
- If a filter policy is configured, only routes passing it can be advertised into the Level-1 area.

Related commands: **import-route (IS-IS view)**.

Examples # Configure the router to redistribute routes from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] import-route isis level-2 into level-1
```

isis

Syntax **isis** [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo isis [*process-id*]

View System view

Parameters *process-id*: Process ID, ranging from 1 to 65535. The default is 1.

vpn-instance-name: VPN instance name, a string of 1 to 31 characters.

Description Use the **isis** command to enable an IS-IS process and an associated VPN instance and enter IS-IS view.

To run IS-IS, you must first use the **isis** command to enable an IS-IS process, then use the **network-entity** command to configure a Network Entity Title (NET) for the router, and then use the **isis enable** command to enable IS-IS on each interface that needs to run the IS-IS process.

Related commands: **isis enable**, **network-entity**.

Examples # Enable IS-IS routing process 1, with the system ID being 0000.0000.0002, and area ID being 01.0001.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 01.0001.0000.0000.0002.00
```

isis authentication-mode

Syntax **isis authentication-mode** { **simple** | **md5** } *password* [**level-1** | **level-2**] [**ip** | **osi**]

undo isis authentication-mode [**level-1** | **level-2**]

View Interface view

Parameters **simple**: Specifies to send the password in plain text.

md5: Specifies to send the password in ciphertext.

password: Specifies a password. For **simple** authentication mode, the *password* must be plain text. For **md5** authentication mode, the password can be either plain text or ciphertext. A plain text password can be a string of up to 16 characters, such as **user918**. A cipher password must be a string of 24 characters, such as **_(TT8F]Y5SQ=^Q'MAF4<1!!**.

level-1: Specifies to set the password for Level-1.

level-2: Specifies to set the password for Level-2.

ip: Specifies the system to check IP related fields in a LSP.

osi: Specifies the system to check OSI related fields in a LSP.

Whether a password should use **ip** or **osi** is not affected by the actual network environment.

This command is not available in loopback interface view.

Description Use the **isis authentication-mode** command to set the IS-IS authentication mode and password for an interface.

Use the **undo isis authentication-mode** command to disable the authentication and remove the password.

There is no password or authentication by default.

If you set a password without specifying any other parameter, the password applies to both Level-1 and Level-2, and the system checks the OSI related fields in a LSP.

Related commands: **area-authentication-mode**, **domain-authentication-mode**.

*The level-1 and level-2 keywords are supported only on an Ethernet or GigabitEthernet interface of a router. Before using the command with the keywords, you need use the **isis enable** command to enable IS-IS on the interface.*

Examples # Set the plain text password easykey for the Serial2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis authentication-mode simple easykey
```

isis circuit-level

Syntax **isis circuit-level** [**level-1** | **level-1-2** | **level-2**]

undo isis circuit-level

View Interface view

Parameters **level-1**: Specifies to set up only level-1 adjacency on the interface.

level-1-2: Specifies to set up level-1-2 adjacency on the interface.

level-2: Specifies to set up only level-2 adjacency on the interface.

Description Use the **isis circuit-level** command to configure link adjacency level for an interface of a level-1-2 router.

Use the **undo isis circuit-level** command to restore the default.

An interface can establish level-1-2 adjacency by default.

This command is only available on a level-1-2 router. You can use it to configure an interface to establish the adjacency of a specified level (**level-1** or **level-2**) with the neighbor, making the interface handle only the specified level hello packets. An interface can receive and send only one level hello packet on a point-to-point link. Using this command can reduce the router's processing time and save bandwidth.

Related commands: **is-level**.

Examples # Suppose serial 2/0 is connected to a non backbone router in the same area. Configure the link adjacency level of serial 2/0 as Level-1 to prevent sending and receiving Level-2 Hello packets.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis enable
[Sysname-Serial2/0] isis circuit-level level-1
```

isis circuit-type

Syntax **isis circuit-type p2p**

undo isis circuit-type

View Interface view

Parameters **p2p**: Specifies the interface's network type as P2P.

Description Use the **isis circuit-type** command to configure the network type for an interface.

Use the **undo isis circuit-type** command to restore the default.

By default, the network type of a router's interface depends on the physical media.

This command is not available in the loopback interface view.

Examples # Configure the network type of the Ethernet1/0 interface as P2P.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] isis enable
[Sysname-Ethernet1/0] isis circuit-type p2p
```

isis cost

Syntax **isis cost** *value* [**level-1** | **level-2**]

undo isis cost [**level-1** | **level-2**]

View Interface view

Parameters *value*: Specifies a cost for SPF calculation on a specified level. The default is 10. The range of cost value differs according to different cost types.

- For types **narrow**, **narrow-compatible** and **compatible**: The cost value ranges from 1 to 63.
- For types **wide** and **wide-compatible**: The cost value ranges from 1 to 16777215.

level-1: Applies the cost to Level-1.

level-2: Applies the cost to Level-2.

Description Use the **isis cost** command to set the link cost of an interface for SPF calculation.

Use the **undo isis cost** command to restore the default.

No cost is configured by default.

If neither **level-1** nor **level-2** is included, the cost applies to both **level-1** and **level-2**.

You are recommended to configure a proper link cost for each interface for optimal route selection.

Relate command: **circuit-cost**.

Examples # Configure the Level-2 link cost as 5 for Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis cost 5 level-2
```

isis dis-name

Syntax **isis dis-name** *symbolic-name*

undo isis dis-name

View Interface view

Parameters *symbolic-name*: Specifies a name for the local LAN, a string of 1 to 64 characters.

Description Use the **isis dis-name** command to configure a name for local LAN. If the local router is the DIS, the name will be advertised in a pseudonode LSP packet.

Use the **undo isis dis-name** command to disable this function.

No name is configured by default.

Note that this command takes effect only on a router with the dynamic hostname process enabled. This command is not supported on a Point-to-Point interface.

This command is not available in the loopback interface view.

Examples # Configure the name as "LOCALAREA" for the local LAN.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] isis dis-name LOCALAREA
```

isis dis-priority

Syntax **isis dis-priority** *value* [**level-1** | **level-2**]

undo isis dis-priority [**level-1** | **level-2**]

View Interface view

Parameters *value*: Specifies a priority for DIS selection from 0 to 127. The default is 64.

level-1: Applies the DIS selection priority to Level-1.

level-2: Applies the DIS selection priority to level-2.

If neither level-1 nor level-2 is specified in this command, the DIS priority applies to both Level-1 and Level-2.

Description Use the **isis dis-priority** command to specify a DIS selection priority on a specified level for an interface.

Use the **undo isis dis-priority** command to restore the default priority of 64.

There is no backup DIS in IS-IS and the router with the 0 priority can also participate in DIS selection.

This command is not available in the loopback interface view.

Examples # Configure the DIS priority on Level-2 as 127 for Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] isis dis-priority 127 level-2
```

isis enable

Syntax **isis enable** [*process-id*]

undo isis enable

View Interface view

Parameters *process-id*: Specifies a IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description Use the **isis enable** command to enable an IS-IS routing process on the interface.

Use the **undo isis enable** command to disable this configuration.

No IS-IS routing process is enabled on an interface by default.

To run IS-IS, you need to use the **isis** command to enable an IS-IS process, and use the **network-entity** command to configure a network entity title (NET) for the router, and then use the **isis enable** command to enable IS-IS on each interface that needs to run the IS-IS process.

Related commands: **isis**, **network-entity**.

Examples # Create IS-IS routing process 1, and enable it on the Serial2/0 interface.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] quit
[Sysname] interface serial2/0
[Sysname-serial2/0] isis enable 1
```

isis mesh-group

Syntax **isis mesh-group** { *mesh-group-number* | **mesh-blocked** }

undo isis mesh-group

View Interface view

Parameters *mesh-group-number*: Specifies a mesh group number from 1 to 4294967295.

mesh-blocked: Blocks the interface from flooding LSPs to make it send LSPs only after receiving requests.

Description Use the **isis mesh-group** command to add the interface into a specified mesh group.

Use the **undo isis mesh-group** command to delete the interface from a mesh group.

An interface is not in any mesh group by default.

For an interface not in a mesh group, it follows the normal process to flood the received LSPs to other interfaces. For the NBMA network with high connectivity and multiple point-to-point links, this will cause repeated LSP flooding and bandwidth waste.

After an interface is added to a mesh group, it will only flood a received LSP to interfaces not belonging to the same mesh group.

When you add an interface to a mesh group or block the interface, make sure to retain some redundancy so that a link failure will not affect the normal LSP packet flooding.

- *A mesh-group is only available for a point-to-point link interface.*
- *This command is not available in loopback interface view.*

Examples # Add the frame relay subinterface Serial2/1.1 to the mesh-group 3.

```
<Sysname> system-view
[Sysname] interface serial 2/1
[Sysname-Serial2/1] link-protocol fr
[Sysname-Serial2/1] quit
[Sysname] interface serial 2/1.1
[Sysname-Serial2/1.1] isis mesh-group 3
```

isis peer-ip-ignore

Syntax **isis peer-ip-ignore**

undo isis peer-ip-ignore

View Interface view

Parameters None

Description Use the **isis peer-ip-ignore** command to configure the PPP interface not to check peer IP address upon receiving Hello packets.

Use the **undo isis peer-ip-ignore** command to restore the default.

By default, the PPP interface checks the peer's IP address upon receiving a hello packet.

An IS-IS PPP interface requires the sender of a hello packet must be on the same network segment with it. Otherwise, it discards the hello packet. You can use the **isis peer-ip-ignore** command to disable this restriction.

Examples

- On a router:

Configure Serial2/0 not to check the peer's IP address of received Hello packets.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis peer-ip-ignore
```

isis enable

Syntax **isis silent**

undo isis silent

View Interface view

Parameters None

Description Use the **isis silent** command to disable the interface from sending and receiving IS-IS hello packets.

Use the **undo isis silent** command to restore the default.

By default, an interface is not disabled from sending and receiving hello packets.

The feature is not supported on the loopback interface.

Examples # Disable Serial 2/0 from sending and receiving hello packets.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis silent
```

isis small-hello

Syntax **isis small-hello**

undo isis small-hello

View Interface view

Parameters None

Description Use the **isis small-hello** command to configure the interface to send small Hello packets without padding field.

Use the **undo isis small-hello** command to disable the feature.

An interface sends standard Hello packets by default.

This command is not available in loopback interface view.

Examples # Configure the serial2/0 interface to send small Hello packets.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis small-hello
```

isis timer csnp

Syntax **isis timer csnp** *seconds* [**level-1** | **level-2**]

undo isis timer csnp [**level-1** | **level-2**]

View Interface view

Parameters *seconds*: Specifies the interval in seconds for sending CSNP packets over broadcast network, ranging from 1 to 600.

level-1: Applies the interval to Level-1.

level-2: Applies the interval to Level-2.

Description Use the **isis timer csnp** command to specify the interval for sending CSNP packets over broadcast network.

Use the **undo isis timer csnp** command to restore the default.

The default CSNP interval is 10 seconds.

- *If no level is specified, the CSNP interval applies to both Level-1 and Level-2 of the current ISIS process. If a level is specified, the interval applies to the level.*
- *This command is not supported on the loopback interface.*
- *This command only applies to the DIS router, which sends CSNP packets periodically.*

Examples # Configure Level-2 CSNP packets to be sent every 15 seconds over the serial2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis timer csnp 15 level-2
```

isis timer hello

Syntax **isis timer hello** *seconds* [**level-1** | **level-2**]

undo isis timer hello [**level-1** | **level-2**]

View Interface view

Parameters *seconds*: Specifies the interval in seconds for sending Hello packets, ranging from 3 to 255.

level-1: Specifies the interval for sending Level-1 Hello packets.

level-2: Specifies the time interval for sending Level-2 Hello packets.

Description Use the **isis timer hello** command to specify the interval for sending hello packets.

Use the **undo isis timer hello** command to restore the default.

The default hello interval is 10 seconds.

- *If no level is specified, the hello interval applies to both Level-1 and Level-2 of the current ISIS process. If a level is specified, the interval applies to the level.*
- *This command is not supported on the loopback interface.*
- *The broadcast link distinguishes between Level-1 and Level-2 packets, so you need specify intervals for the two levels respectively. The point-to-point link however does not distinguish, so you need not specify intervals respectively.*
- *As the shorter the interval is, the more system resources will be occupied, you should configure a proper interval as needed.*

Related commands: **isis timer holding-multiplier**.

Examples # Configure Level-2 Hello packets to be sent every 20 seconds over the serial2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] isis timer hello 20 level-2
```

isis timer holding-multiplier

Syntax **isis timer holding-multiplier** *value* [**level-1** | **level-2**]

undo isis timer holding-multiplier [**level-1** | **level-2**]

View Interface view

Parameters *value*: Number of hello intervals, in the range of 3 to 1000.

level-1: Applies the number to the Level-1 IS-IS neighbor.

level-2: Applies the number to the Level-2 IS-IS neighbor.

- *If neither level-1 nor level-2 is specified in the command, the number applies to the current level IS-IS process.*
- *This command is not available in loopback interface view.*

Description Use the **isis timer holding-multiplier** command to configure the number of hello intervals, within which if the interface receive no hello packets, its neighbor is considered dead.

Use the **undo isis timer holding-multiplier** command to restore the default.

On an interface, the default number of hello intervals is three.

You can specify the number of hello intervals for Level-1 and Level-2 neighbors respectively on a broadcast network. For a point-to-point link, there is only one kind of Hello packet, so you need not specify Level-1 or Level-2.

The specified number of hello intervals is used to configure the Holddown time. If a router receives no Hello packets from a neighbor within Holddown time, it will take the neighbor as dead. The Holddown time can be configured differently for different routers within an area. You can adjust the Holddown time by changing either the hello interval or the number of Hello intervals on an interface.

Related commands: **isis timer hello**.

Examples # Configure the number of Level-2 Hello intervals as 6 for interface serial2/0, that is, if no hello packet is received from the interface within 6 hello intervals, its neighbor is considered dead.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial 2/0] isis timer holding-multiplier 6 level-2
```

isis timer lsp

Syntax **isis timer lsp** *time* [**count** *count*]

undo isis timer lsp

View Interface view

Parameters *time*: Specifies the minimum interval in milliseconds for sending link-state packets, ranging from 1 to 1000.

count: Specifies the maximum number of link-state packets to be sent at one time, in the range of 1 to 1000. The default is 100 for the broadcast interface and 11 for point-to-point interface.

Description Use the **isis timer lsp** command to configure the interval for sending link-state packets on the interface.

Use the **undo isis timer lsp** command to restore the default of 33ms.

Related commands: **isis timer retransmit**.

This command is not available in loopback interface view.

Examples # Configure the interval as 500 milliseconds for sending LSPs on interface serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] isis timer lsp 500
```

isis timer retransmit

Syntax **isis timer retransmit** *seconds*

undo isis timer retransmit

View Interface view

Parameters *seconds*: Specifies the interval in seconds for retransmitting LSP packets, ranging from 1 to 300.

Description Use the **isis timer retransmit** command to configure the interval for retransmitting LSP packets over point-to-point link.

Use the **undo isis timer retransmit** command to restore the default of 5s.

You need not use this command over a broadcast link where no LSP response is required.

Related commands: **isis timer lsp**.

- *This command is not available in loopback interface view.*
- *Configure a proper time to avoid unnecessary retransmissions.*

Examples # Configure the LSP retransmission interval as 10 seconds for the serial2/0 interface.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] isis timer retransmit 10
```

is-level

Syntax **is-level** { **level-1** | **level-1-2** | **level-2** }

undo is-level

View IS-IS view

Parameters **level-1**: Configures the router to work on Level-1, which means it only calculates routes within the area, and maintains the L1 LSDB.

level-1-2: Configures the router to work on Level-1-2, which means it calculates routes and maintains the LSDBs for both L1 and L2.

level-2: Configures the router to work on Level-2, which means it calculates routes and maintains the LSDB for L2 only.

Description Use the **is-level** command to configure IS-IS router type.

Use the **undo is-level** command to restore the default.

The default router type is **level-1-2**.

It is recommended to configure system level when you configure IS-IS.

You can configure all the routers as either Level-1 or Level-2 if there is only one area, because there is no need for all routers to maintain two identical databases at the same time. In this case, you are recommended to configure all the routers as Level-2 in the IP network for scalability consideration.

Related commands: **isis circuit-level**.

Examples # Configure the router to work in Level-1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-level level-1
```

is-name

Syntax **is-name** *sys-name*

undo is-name

View IS-IS view

Parameters *symbolic-name*: Specifies a name for the local IS, a string of 1 to 64 characters.

Description Use the **is-name** command to enable the dynamic hostname process and configure a name for the router, which is advertised in an LSP.

Use the **undo is-name** command to remove the configuration.

No IS name is configured by default.

Examples # Configure a name for the local IS.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name RUTA
```

is-name map

Syntax **is-name map** *sys-id map-sys-name*

undo is-name map *sys-id*

View IS-IS view

Parameters *sys-id*: System ID or a pseudonode ID of a remote IS.

map-sys-name: Specifies a name for the remote IS, a string of 1 to 64 characters.

Description Use the **is-name map** command to map a name to a remote IS. Each remote IS system ID corresponds to only one name.

Use the **undo is-name map** command to remove the configuration.

By default, no name is configured for a remote IS.

Examples # Map the name RUTB to the remote IS 0000.0000.0041.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-name map 0000.0000.0041 RUTB
```

is-snmp-traps enable

Syntax **is-snmp-traps enable**

undo is-snmp-traps

View IS-IS view

Parameters None

Description Use the **is-snmp-traps enable** command to enable the SNMP Trap function of IS-IS.

Use the **undo is-snmp-traps** command to disable this function.

SNMP Trap is enabled by default.

Examples # Enable SNMP Trap.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] is-snmp-traps enable
```

log-peer-change (IS-IS view)

Syntax **log-peer-change**

undo log-peer-change

View IS-IS view

Parameters None

Description Use the **log-peer-change** command to enable logging on IS-IS adjacency state changes.

Use the **undo log-peer-change** command to disable the logging.

The feature is enabled by default.

After the feature is enabled, information about IS-IS adjacency state changes is sent to the configuration terminal.

Examples # Enable logging on the IS-IS adjacency state changes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] log-peer-change
```

lsp-fragments-extend

Syntax **lsp-fragments-extend** [[**level-1** | **level-2** | **level-1-2**] | [**mode-1** | **mode-2**]] *

undo lsp-fragments-extend

View IS-IS view

Parameters **mode-1**: Fragment extension mode 1, used on a network where some routers do not support LSP fragment extension.

mode-2: Fragment extension mode 2, used on a network where all routers support LSP fragment extension.

level-1: Applies the fragment extension mode to Level-1 LSPs.

level-2: Applies the fragment extension mode to Level-2 LSPs.

level-1-2: Applies the fragment extension mode to both Level-1 and Level-2 LSPs.

*The **mode-1** and **level-1-2** keywords are used by default.*

Description Use the **lsp-fragments-extend** command to enable LSP fragment extension in a specified mode and level.

Use the **undo lsp-fragments-extend** command to disable this feature.

The feature is disabled by default.

Note the following:

- After LSP fragment extension is enabled in an IS-IS process, the MTUs of all the interfaces on which this IS-IS process is enabled must not be less than 512; otherwise, LSP fragment extension will not take effect.
- At least one virtual system needs to be configured for the router to generate extended LSP fragments. An IS-IS process allows 50 virtual systems at most.

Examples # Enable LSP fragment extension of **mode-1** and **Level-2**.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-fragments-extend mode-1 level-2
```

lsp-length originate

Syntax **lsp-length originate** *size* [**level-1** | **level-2**]

undo lsp-length originate [**level-1** | **level-2**]

View IS-IS view

Parameters *size*: Specifies the maximum size in bytes of a LSP packet, ranging from 512 to 16384.

level-1: Applies the size to Level-1 LSP packets.

level-2: Applies the size to Level-2 LSP packets.

If neither Level-1 nor Level-2 is specified in the command, the configured maximum size applies to the current IS-IS level.

Description Use the **lsp-length originate** command to configure the maximum size of generated Level-1 or Level-2 LSPs.

Use the **undo lsp-length originate** command to restore the default.

The maximum size of 1497 bytes is the default.

Examples # Configure the maximum size of the generated Level-2 LSPs as 1024 bytes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length originate 1024 level-2
```

lsp-length receive

Syntax **lsp-length receive** *size*

undo lsp-length receive

View IS-IS view

Parameters *size:* Maximum size of received LSPs, in the range of 512 to 16384 bytes.

Description Use the **lsp-length receive** command to configure the maximum size of received LSPs.

Use the **undo lsp-length receive** command to restore the default.

By default, the maximum size of received LSPs is 1497 bytes.

Examples # Configure the maximum size of received LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] lsp-length receive 1024
```

maximum load-balancing (IS-IS view)

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View IS-IS view

Parameters *number*: Maximum number of equal-cost load balanced routes, in the range 1 to 8.

Description Use the **maximum load-balancing** command to configure the maximum number of equal-cost load balanced routes.

Use the **undo maximum load-balancing** command to restore the default.

The maximum number varies by device.

Examples # Configure the maximum number of equal-cost load-balanced routes as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-isis-100] undo maximum load-balancing
```

network-entity

Syntax **network-entity** *net*

undo network-entity *net*

View IS-IS view

Parameters *net*: Network Entity Title (NET) in the format of X...X.XXXX....XXXX.00, with the first part X...X being the area address, the middle part XXXX....XXXX (a total of 12 "X") being the router's system ID and the last part 00 being SEL.

Description Use the **network-entity** command to configure the Network Entity Title for an IS-IS routing process.

Use the **undo network-entity** command to delete a NET.

No NET is configured by default.

A NET is a network service access point (NSAP), and it is in the range of 8 to 20 bytes for IS-IS.

A NET has three parts: The first part is area ID, which ranges from 1 to 13 bytes. Routers in the same area must have the same area ID. The second part is the router's 6-byte system ID, which is unique within the whole area and backbone area. The third part is the 1-byte SEL that must be 00. Generally, a router needs one NET. In the case of repartitioning an area, such as merging or splitting, you can configure multiple NETs beforehand for the router to ensure correct and continuous routing.

Related commands: **isis**, **isis enable**.

Examples # Specify the NET as 10.0001.1010.1020.1030.00, of which 10.0001 is the area ID and 1010.1020.1030 is the system ID.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
```

preference (IS-IS view)

Syntax **preference** { **route-policy** *route-policy-name* | *preference* } *

undo preference

View IS-IS view

Parameters *preference*: Specifies the preference for IS-IS protocol, ranging from 1 to 255. *route-policy-name*: Routing policy name, a string of 1 to 19 characters. The preference applies to routes passing the routing policy.

Description Use the **preference** command to configure the preference for IS-IS protocol.

Use the **undo preference** command to restore the default.

By default, the IS-IS protocol preference is 15.

If a routing policy is specified in this command, the preference (if any) set by the routing policy applies to those matched routes. Other routes use the preference set by the **preference** command.

When a router runs multiple routing protocols at the same time, the system will set a preference to each routing protocol. If several protocols find routes to the same destination, the route of the routing protocol with the highest preference is selected.

Examples # Configure the preference of IS-IS protocol as 25.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] preference 25
```

reset isis all

Syntax **reset isis all** [*process-id* | **vpn-instance** *vpn-instance-name*]

View User view

Parameters *process-id*: Clears the data structure information of an IS-IS process numbered from 1 to 65535.

vpn-instance-name: Clears the data structure information of a VPN instance named with a string of 1 to 31 characters.

Description Use the **reset isis all** command to clear all ISIS data structure information.

No data structure information is cleared by default.

This command is used when the LSP needs to be updated immediately. For example, after performing the **area-authentication-mode** and **domain-authentication-mode** commands, you can use this command to clear old LSPs.

Related commands: **area-authentication-mode**, **domain-authentication-mode**.

Examples # Clear all IS-IS data structure information.

```
<Sysname> reset isis all
```

reset isis peer

Syntax **reset isis peer** *system-id* [*process-id* | **vpn-instance** *vpn-instance-name*]

View User view

Parameters *system-id*: Specifies the system ID of an IS-IS neighbor.

process-id: Specifies the ID of an IS-IS process, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **reset isis peer** command to clear the data structure information of a specified IS-IS neighbor.

The command is disabled by default.

This command is used when you need to re-establish an IS-IS neighbor.

Examples # Clear the data structure information of the neighbor with system ID being 0000.0c11.1111.

```
<Sysname> reset isis peer 0000.0c11.1111
```

set-overload

Syntax **set-overload** [**on-startup start-from-nbr** *system-id* [*timeout* [*nbr-timeout*]]] [**allow** { **interlevel** | **external** } *]

undo set-overload

View IS-IS view

Parameters **on-startup**: Specifies to start the overload tag timeout timer upon system startup.

start-from-nbr *system-id*: Specifies to start the overload tag timeout timer when the router begins to establish the connection with a neighbor.

timeout: Specifies the overload tag timeout timer, with an interval from 5 to 86400 seconds. The timer is started after system startup. The default is 600 seconds.

nbr-timeout: Specifies the overload tag timeout timer that is started when the router begins to establish the connection with a neighbor after system startup. The time has an interval from 5 to 86400 seconds. The default is 1200 seconds.

allow: Specifies to allow advertising address prefixes. By default, no address prefixes are allowed to be advertised when the system is in overload state.

interlevel: Allows advertising IP address prefixes learnt from different IS-IS levels with the **allow** keyword specified.

external: Allows advertising IP address prefixes learnt from other routing protocols with the **allow** keyword specified.

Description Use the **set-overload** command to set the overload tag for the current router.

Use the **undo set-overload** command to clear the overload tag.

No overload flag is set by default.

When the overload flag is set for a router, the routes calculated by the router will be ignored by other routers when they calculate SPF. (But the routes directly connected to the router will not be ignored.)

When a router is set overload tag, other routers will not send packets to the router for forwarding.

Examples # Set overload flag on the current router.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] set-overload
```

spf-slice-size

Syntax **spf-slice-size** *duration-time*

undo spf-slice-size

View IS-IS view

Parameters *duration-time*: Specifies the duration in milliseconds of each sliced SPF calculation, ranging from 10 to 50000. Each sliced SPF calculation is ended when the duration time is reached. If the *duration-time* is set to 0, the entire SPF calculation will not be sliced.

Description Use the **spf-slice-size** command to specify the duration for each sliced SPF calculation.

Use the **undo spf-slice-size** command to restore the default.

The default SPF calculation duration is 10 milliseconds.

To prevent the SPF calculation from occupying the system resources for a long time, you can use this command to slice the whole SPF calculation into pieces.

You are not recommended to change the default setting.

Examples # Set the duration of each sliced SPF calculation to 1 second.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] spf-slice-size 1000
```

summary (IS-IS view)

Syntax **summary** *ip-address* { *mask* | *mask-length* } [**avoid-feedback** | **generate_null0_route** | **tag** *tag* | [**level-1** | **level-1-2** | **level-2**]] *

undo summary *ip-address* { *mask* | *mask-length* } [**level-1** | **level-1-2** | **level-2**]

View IS-IS view

Parameters *ip-address*: Destination IP address of a summary route.

mask: Mask of the destination IP address, in dotted decimal format.

mask-length: Mask length, in the range of 0 to 32.

avoid-feedback: Specifies to avoid learning aggregate routes by routing calculation.

generate_null0_route: Specifies to generate the Null 0 route to avoid routing loops.

tag *tag*: Specifies a management tag, in the range of 1 to 4294967295.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to the Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to the Level-2 area.

Description Use the **summary** command to configure a summary route.

Use the **undo summary** command to remove a summary route.

No summarization is configured by default.

If no level is specified, only the **level-2** routes will be summarized by default.

You can summarize multiple contiguous networks with a summary network to reduce the size of the routing table, as well as that of LSP and LSDB generated by the router. It is allowed to summarize native IS-IS routes and redistributed routes. After summarization, the cost of the summary route is the smallest cost of those summarized routes.

Note that the router summarizes only routes in local LSPs.

Examples # Configure a summary route 202.0.0.0/8.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] summary 202.0.0.0 255.0.0.0
```

timer isp-generation

Syntax **timer lsp-generation** *maximum-interval* [*initial-interval* [*incremental-interval*]] [**level-1** | **level-2**]

undo timer lsp-generation [**level-1** | **level-2**]

View IS-IS view

Parameters *maximum-interval*: Maximum interval in seconds for generating ISIS LSPs, in the range 1 to 120.

initial-interval: Initial interval in milliseconds for generating ISIS LSPs, in the range 10 to 60000. The default is 0.

incremental-interval: Incremental interval (in milliseconds), in the range 10 to 60000. The default is 0.

level-1: Applies the specified intervals to generating level-1 LSPs.

level-2: Applies the specified intervals to generating level-1 LSPs.

Description Use the **timer lsp-generation** command to specify intervals for ISIS LSP generation.

Use the **undo timer isp-generation** command to restore the default.

By default, the LSP generation interval is 2 seconds.

- *If only the maximum interval is specified, this maximum interval is the LSP generation interval.*
- *If both the maximum and initial intervals are specified, the system can adjust the LSP generation interval upon topology changes. When the topology is stable, the initial interval applies as the LSP generation interval. When topology changes become frequent, the LSP generation interval is the maximum or initial interval.*
- *If all the maximum, initial and incremental intervals are specified, the system will adjust the LSP generation interval upon topology changes in this way: when the network changes are infrequent, the initial interval applies as the LSP generation interval. When the network changes become frequent, the generation interval changes between the initial and maximum intervals based on the specified incremental interval.*

By using this command to adjust the LSP generation interval, you can save the bandwidth and router resources that may be wasted due to frequent network changes.

Examples # Set the maximum LSP generation interval to 10 seconds, initial interval to 100 milliseconds and the incremental interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 10 100 200
```

Set the maximum LSP generation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer lsp-generation 15
```

timer lsp-max-age

Syntax **timer lsp-max-age** *seconds*

undo timer lsp-max-age

View IS-IS view

Parameters *seconds*: Specifies the LSP maximum aging time in seconds, ranging from 1 to 65535.

Description Use the **timer lsp-max-age** command to set the LSP maximum aging time for the current router.

Use the **undo timer lsp-max-age** command to restore the default.

The default is 1200 seconds.

A router puts the specified LSP maximum aging time into an LSP before advertisement. When the LSP is received by other routers, the aging time will decrease as the time goes by. If no update is received for the LSP after its aging time decreases to 0, the LSP will be deleted from the LSDB.

Related commands: **timer lsp-refresh**.

Examples # Set the maximum LSP aging time to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-max-age 1500
```

timer lsp-refresh

Syntax **timer lsp-refresh** *seconds*

undo timer lsp-refresh

View IS-IS view

Parameters *second*s: Specifies the LSP refresh interval in seconds, ranging from 1 to 65534.

Description Use the **timer lsp-refresh** command to set the LSP refresh interval.

Use the **undo timer lsp-refresh** to restore the default.

The default is 900 seconds.

Using this feature, you can keep LSPs in synchronization for the whole area.

Related commands: **timer lsp-max-age**.

*To refresh LSPs before they are aged out, the interval set by the **timer lsp-refresh** command must be smaller than that set by the **timer lsp-max-age** command.*

Examples # Set the LSP refresh interval to 1500 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] timer lsp-refresh 1500
```

timer spf

Syntax **timer spf** *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo timer spf

View IS-IS view

Parameters *maximum-interval*: Specifies the maximum interval (in seconds) for SPF calculations, ranging from 1 to 120.

minimum-interval: Specifies the minimum interval (in milliseconds) for SPF calculations, ranging from 10 to 60000.

incremental-interval: Specifies the incremental interval (in milliseconds) for SPF calculations, ranging from 10 to 60000.

Description Use the **timer spf** command to set the time intervals for ISIS routing calculation.

Use the **undo timer spf** command to restore the default.

The default IS-IS SPF calculation interval is 10 seconds.

When the network changes are infrequent, the SPF calculation interval decreases to the minimum interval. When the network changes become frequent, the calculation interval is increased by *inc-interval*$*(2^{n-2})$, (n is the number of network changes that triggered SPF calculations) until the maximum interval is reached.

With this feature, you can prevent the router from over consumption due to frequent network changes.

Examples # Set the maximum SPF calculation interval to 10 seconds, minimum interval to 100 milliseconds and the incremental interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 10 100 200
```

Set the maximum SPF calculation interval to 15 seconds.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]timer spf 15
```

virtual-system

Syntax **virtual-system** *virtual-system-id*

undo virtual-system *virtual-system-id*

View IS-IS view

Parameters *virtual-system-id*: Virtual system ID of the IS-IS process.

Description Use the **virtual-system** command to configure a virtual system ID for the IS-IS process. No extended LSPs are generated without the virtual system ID.

Use the **undo virtual-system** command to remove the virtual system ID.

Up to 50 virtual system IDs can be configured for the IS-IS process.

Examples # Set a virtual system ID of 2222.2222.2222 for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] virtual-system 2222.2222.2222
```

75 IS-IS DEBUGGING COMMANDS

debugging isis

Syntax **debugging isis** { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **event** | **general-error** | **graceful-restart** | **ha-events** | **interface-information** | **memory-allocating** | **miscellaneous-errors** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **traffic-eng** { **advertisement** | **event** } | **update-packet** } [*process-id* | [**vpn-instance** *vpn-instance-name*]]

undo debugging isis { **adjacency** | **all** | **authentication-error** | **checksum-error** | **circuit-information** | **configuration-error** | **datalink-receiving-packet** | **datalink-sending-packet** | **event** | **general-error** | **graceful-restart** | **ha-events** | **interface-information** | **memory-allocating** | **miscellaneous-errors** | **receiving-packet-content** | **self-originate-update** | **sending-packet-content** | **snp-packet** | **spf-event** | **spf-summary** | **spf-timer** | **task-error** | **timer** | **traffic-eng** { **advertisement** | **event** } | **update-packet** } [*process-id* | [**vpn-instance** *vpn-instance-name*]]

View User view

Default Level 1: Monitor level

Parameters **adjacency**: Enables IS-IS adjacency debugging.

all: Enables all IS-IS debugging.

authentication-error: Enables debugging for authentication errors.

checksum-error: Enables debugging for IS-IS LSP checksum errors.

circuit-information: Enables debugging for the IS-IS-enabled interfaces.

configuration-error: Enables debugging for configuration errors.

datalink-receiving-packet: Enables debugging for data link-layer packet receiving.

datalink-sending-packet: Enables debugging for data link-layer packet sending.

event: Enables IS-IS event debugging.

general-error: Enables debugging for IS-IS errors.

graceful-restart: Enables debugging for IS-IS GR.

ha-events: Enables debugging for data hot backup. This keyword takes effect only on a distributed device.

interface-information: Enables IS-IS interface debugging.

memory-allocating: Enables debugging for IS-IS memory allocation.

miscellaneous-errors: Enables debugging for errors unrelated to IS-IS.

receiving-packet-content: Enables debugging for received IS-IS packet contents.

self-originate-update: Enables debugging for IS-IS local updates.

sending-packet-content: Enables debugging for sent IS-IS packet contents.

snp-packet: Enables IS-IS SNP packet debugging.

spf-event: Enables debugging for IS-IS SPF route calculation.

spf-summary: Enables debugging for IS-IS route calculation summary.

spf-timer: Enables debugging for IS-IS route calculation triggers.

task-error: Enables debugging for IS-IS task errors.

timer: Enables IS-IS timer debugging.

traffic-eng: Enables debugging for IS-IS traffic switch fabricering.

advertisement: Enables debugging for IS-IS traffic switch fabricering advertisement.

event: Enables debugging for IS-IS traffic switch fabricering events.

update-packet: Enables IS-IS update packet debugging.

process-id: IS-IS process ID, in the range of 1 to 65535.

vpn-instance-name: Specifies a VPN instance name, a string of 1 to 31 characters. Support for this argument varies with device models.

Description

Use the **debugging isis** command to enable specified debugging for IS-IS. Use the **undo debugging isis** command to disable specified debugging for IS-IS.

Table 243 Description on the fields of the debugging isis adjacency command

Field	Description
Circuit State Up Success	Interface is up.
Circuit State Down Success	The interface is down (The adjacency processing was complete).

Table 243 Description on the fields of the debugging isis adjacency command

Field	Description
Rxed *helloType* Hello on *circuitName*, from SNPA *SNPA*	IS-IS received a hello packet. *helloType*: Hello packet type: Lan L1, Lan L2, or P2P. *circuitName*: Interface name *SNPA*: Source MAC address of the packet.
Sending *helloType* Hello on *circuitName*	IS-IS is sending a hello packet. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P. *circuitName*: Interface name
Running DIS Election, *circuitName*	IS-IS is running a DIS election. *circuitName*: Interface name
Declaring as DIS,DIS Type *type*,on *circuitName*, Old DIS (*net1*), New DIS *net2*	IS-IS is declaring the new DIS. type: L1 or L2. *net1: Net entity title of the old DIS.* net2: Net entity title of the new DIS.
Send Failure	Sending a hello packet failed.
Update DIS Down Processing Failure	Processing the DIS Down event failed.
Circuit State change reported for Unknown Circuit Type	Interface type change error due to unknown interface type
Adjacency(s) Not deleted On circuit Down	Adjacency deletion failed after the interface was down.
Rxed P2P IIH on *circuitName*.IIH Rejected Wrong Circ Type(*circuitType*)	The received hello packet was rejected because the interface type (point-to-point) is wrong. *circuitName*: Interface name *circuitType*: Interface type, which can be L1, L2, or L12.
helloType IIH request reserved circuit type. Ignored	IS-IS received an IIH packet with interface type as reserved and therefore ignored it. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.
Rxed *helloType* IIH with duplicate Local System ID. IIH Discarded	The received hello packet was not processed due to a duplicate system ID. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.
helloType IIH Authentication Failure. IIH Discarded	The received hello packet was discarded due to an authentication failure. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.
Rxed *helloType* IIH has Invalid IP address.IIH Ignored	IP address is invalid; therefore, the received hello packet was not processed. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.
Rxed *helloType* IIH contains No usable Ip Address. IIH Discarded	The received hello packet was discarded because it contains no usable IP address. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.

Table 243 Description on the fields of the debugging isis adjacency command

Field	Description
Rxed *helloType* IIH on *circuitName* contains Duplicate Ip Address. IIH Discarded	The received hello packet was discarded because it contains a duplicate IP address. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P. *circuitName*: Interface name
Rxed *helloType* IIH on % *circuitName* contains Duplicate Ipv6 Address. IIH Discarded	The received hello packet was discarded because it contains a duplicate IPv6 address. *helloType*: PDU packet type: LAN L1, LAN L2, or P2P. *circuitName*: Interface name
Rxed Serial IIH on *circuitName*, Protocol supported mismatch. IIH Discarded	The received hello packet was discarded due to a protocol mismatch. *circuitName*: Interface name
Rxed P2P IIH on % *circuitName* contains no Protocol Support at all. IIH Ignored	The received hello packet was discarded due to no protocol support. *circuitName*: Interface name
Rxed Ethernet IIH on *circuitName*. Ignored	The received Ethernet IIH packet was discarded because the interface type is not broadcast. *circuitName*: Interface name
helloType Level Mismatch.Local Level *circuitLevel*	Packet type mismatch *helloType*: Hello packet type: LAN L1, LAN L2, or P2P. *circuitLevell*: Current level of the link. It can be L1, L2, or L12.
helloType, No common protocol supported	The received hello packet matched no protocol. *helloType*: Hello packet type: LAN L1, LAN L2, or P2P.
Rxed LAN IIH from system : %*systemId*	IS-IS received an Ethernet IIH packet. *systemId*: System ID of the sending device.
Rxed P2P IIH from system : %*systemId*	IS-IS received a P2P IIH packet. *systemId*: System ID of the sending device.
Rxed ISH from system : %*systemId*	IS-IS received an ISH packet. *systemId*: System ID of the sending device.

Table 244 Description on the fields of the debugging isis authentication-error command

Field	Description
For all processes of the VPN instance *vpn-instance-name*, Indication of authentication errors debugging is on	The authentication error debugging is enabled for all the IS-IS processes of the VPN instance.
For the process *process-id*, Indication of authentication errors debugging is on	The authentication error debugging is enabled for the IS-IS process.

Table 245 Description on the fields of the debugging isis checksum-error command

Field	Description
For all processes of the VPN instance *vpn-instance-name* , IS-IS Checksum errors debugging is on	The LSP checksum error debugging is enabled for all the IS-IS processes of the VPN instance.
For the process *process-id*, IS-IS Checksum errors debugging is on	The LSP checksum error debugging is enabled for the IS-IS process.

Table 246 Description on the fields of the debugging isis circuit-information command

Field	Description
% *circuitName* not enabled for Ipv4	IPv4 is not enabled on the interface. *circuitName*: Interface name
% *circuitName* not enabled for Ipv6	IPv6 is not enabled on the interface. *circuitName*: Interface name
% *circuitName* not enabled	IS-IS is not enabled on the interface. *circuitName*: Interface name
Interface MTU should not be too small(< 131)	Interface MTU cannot be smaller than 131.
The IP is set to UP for IS-IS on interface	IP of the IS-IS enabled interface is up.
The IP is set to DOWN for IS-IS on interface	IP of the IS-IS enabled interface is down.
The IP is set to UP for ISISv6 on interface	IP of the IS-ISv6 enabled interface is up.
The IP is set to DOWN for ISISv6 on interface	IP of the IS-ISv6 enabled interface is down.
CIRC: Circ Up not processed. Circuit already up	The interface is already UP; therefore, no more interface UP requests are processed.
CIRC: Circ Down not processed. Circuit already Down	The interface is already DOWN; therefore, no more interface DOWN requests are processed.
CIRC: Join AllIS multicast address error	An error occurred while the interface was joining all the multicast groups.
CIRC: Join ALLL1IS multicast address error	An error occurred while the interface was joining L1 multicast groups.
CIRC: Join ALLL2IS multicast address error	An error occurred while the interface joined L2 multicast groups.
CIRC: Leave ALLL1IS multicast address error	An error occurred while the interface was leaving L1 multicast groups.
CIRC:Leave ALLL2IS multicast address error	An error occurred while the interface was leaving L2 multicast groups.
CIRC: Leave ALLIS multicast address error	An error occurred while the interface was leaving all the multicast groups.
CIRC : *circuitName* not enabled	IS-IS is not enabled on the interface. *circuitName*: Interface name
CIRC: Circuit *circuitName* is on wrong state while enabling	An error occurred when IS-IS was enabled on the interface. *circuitName*: Interface name
CIRC : *circuitName* not enabled for Circuit Type Change	The interface was not enabled with IS-IS when interface state changed. *circuitName*: Interface name

Table 247 Description on the fields of the debugging isis datalink-receiving-packet command

Field	Description
Circuit NOT operationally ON	Interface is not ready for operation.
SYS not functional. Ignoring recvd packet	System is not functioning and therefore ignores the received packets.
Rxed IS-IS PDU on Circuit *circuitName*, PDU's type is *packetType*	An IS-IS PDU was received on the interface. *circuitName*: Interface name *packetType*: Interface type.

Table 248 Description on the fields of the debugging isis datalink-sending-packet command

Field	Description
Sending IS-IS PDU on Circuit *circuitName*	Sending IS-IS PDU through the interface. *circuitName*: Interface name
Socket Send PDU error	An error occurred when the socket was sending a PDU.
Socket Send PDU success	Socket sent a PDU successfully.
Sending IS-IS PDU Failure	Socket failed to send a PDU.

Table 249 Description on the fields of the debugging isis general-error command

Field	Description
UPDT: PDU length mismatch in SNP: RecLen = %d, EncodeLen = %d.	SNP packet length mismatch
RECV: PDU length mismatch in Hello PDU : RecLen = %d, EncodeLen = %d	Hello packet length mismatch
PROT-ERR: Wrong P2P IIH Hdr Length, %d. It should be %d	Wrong P2P Hello packet header length
PROT-ERR: Wrong LAN IIH Hdr Length, %d. It should be %d	Wrong LAN Hello packet header length
PROT-ERR: Wrong L1/2CSNP Hdr Length, %d. It should be %d	Wrong L1/2 CSNP packet header length
PROT-ERR: Wrong L1/2 PSNP Hdr Length, %d. It should be %d	Wrong L1/2 PSNP packet header length
PROT_ERR: Wrong L1/2 LSP Hdr Length, %d. It should be %d	Wrong L1/2 LSP packet header length

Table 250 Description on the fields of the debugging isis graceful-restart command

Field	Description
RST: *levelType* T1 Timer Started on *circName*, Counter: *count*	GR timer started. *levelType*: system type, which can be L1 or L2. *count*: Number of times GR timer has started. *circName*: Interface name
RST: Notifying RM that the Process is Entering Restart.	Notifying RM that the process is entering the GR state.
RST: Notifying RM that the Process is Leaving Restart (Due to Rst Disable).	Notifying RM that the process is leaving the GR state because GR is disabled.

Table 250 Description on the fields of the debugging isis graceful-restart command

Field	Description
RST: *levelType* T1 Timer Expired on *circName*, Counter: *count*	GR timer expired. *levelType*: system type, which can be L1 or L2. *count*: Number of times GR timer has started. *circName*: Interface name
RST: Restart COMPLETE in *millisecond* ms	GR is complete. *millisecond*: Length of GR duration in milliseconds.

Table 251 Description on the fields of the debugging isis ha-events command

Field	Description
HSB-SMOOTH: Circuit *circuitName* is on wrong state while enabling	An error occurred while the interface was being enabled during the smoothing.
HSB-SMOOTH: Processing the circuit join multicast group error	An error occurred while the interface was joining the multicast group in the smoothing.
HSB-SMOOTH: Circuit *circuitName* not Consistent with RM/RM6.	The current interface is inconsistent with RM/RM6 in the smoothing.
HSB-SMOOTH: Update module processing the circuit down error	The update module failed to process the interface Down event in the smoothing.
HSB-SMOOTH: Update module processing the circuit up error	The update module failed to process the interface Up event in the smoothing.
HSB-SMOOTH: Failed to start Max LspGen timer	Starting the maximum LSP generation interval timer failed in the smoothing.
HSB-SMOOTH: LSP Expired. Purging LSP	LSP expired in the smoothing; therefore, the LSP was being deleted.
HSB-SMOOTH: While LSDB Smoothing, Failed to Start Lsp age timer	Starting LSP age timer failed in LSDB smoothing.
HSB-SMOOTH: Batch Backup was Not Complete : Resetting ISIS	Batch backup was not complete in the smoothing; therefore, IS-IS is being reset.
Length : length	Real-time backup message length

Table 252 Description on the fields of the debugging isis interface-information command

Field	Description
CIRC: MTU Size Exceeds Max PDU Size mtuSize, Setting it to Max PDU Size.	The interface MTU exceeds the maximum PDU size; therefore, the interface MTU is being set to the maximum PDU size.
IF: Disable ip route isis Failed	Disabling IP routing on the interface failed.
IF:Can't get the interface index	IS-IS cannot obtain the interface index.
IF:Can't get the interface type	IS-IS cannot obtain the interface type.
ISIS interface IPV4/V6 Addr nums exceed array maxnum	The number of IPv4/IPv6 IP addresses on the interface has exceeded the upper limit.

Table 253 Description on the fields of the debugging isis receiving-packet-content command

Field	Description
Rxed *pduLevel* CSNP From *sourceId* (*circuitName*).	IS-IS received a CSNP packet. *pduLevel*: L1 or L2. *sourceId*: Source NSAP address of the CSNP packet. *circuitName*: Name of the interface through which the CSNP packet was received.
** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **	Contents in the CSNP packet, including the header, LSP entries, and Authentication Information field.
Rxed *pduLevel* PSNP From *sourceId* (*circuitName*).	IS-IS received a PSNP packet. *pduLevel*: L1 or L2. *sourceId*: Source NSAP address of the PSNP packet. *circuitName*: Name of the interface through which the PSNP packet was received.
** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** ** **	Contents in the corresponding PSNP packet, including the header, LSP entries, and Authentication Information field.

Table 254 Description on the fields of the debugging isis self-originate-update command

Field	Description
UPDT: RESET REQUIRED.	The IS-IS process needs to be reset.
UPDT: Circuit IPv4/IPv6 Up *circName*	Local interface is up (IPv4/IPv6). *circName*: Interface name.
UPDT: Circuit IPv4/IPv6 Down *circName*	Local interface is down (IPv4/IPv6). *circName*: Interface name
UPDT: Circuit Cost change process failed	Changing the local interface cost failed.
UPDT: Circuit Ipv4/v6 Addr add *ipAddress*	The IPv4/IPv6 address was added to the interface. *ipAddress*: Interface IP address.
UPDT: Circuit Ipv4/v6 Addr Del *ipAddress*	The IPv4/IPv6 address was deleted from the interface. *ipAddress*: Interface IP address.
UPDT: Rxed *levelType* Default cost Change	The default cost of the local interface changed. *levelType*: Interface level type, which can be L1 or L2.
INTELLITMR: Starting a *lspLevel* LSP Timer for LSP Generation.	IS-IS started the LSP generation timer. *lspLevel*: LSP type, which can be L1 or L2.
UPDT: Filling of Auth data in Lsp failed	Filling authentication information in the locally originated LSP failed.
UPDT: Creation of Zero lsp Desc failed	Creating local zero LSP fragment failed.
UPDT: Adding Ipv4/v6 Address *ipAddress* into *pduLevel* LSPs	The IP address was being added to the local LSPs.
UPDT: Adding in the LSP Neighbor option, TLV 22	The neighbor TLV was added to the local LSP.

Table 254 Description on the fields of the debugging isis self-originate-update command

Field	Description
UPDT: Adding Redist Address *ipAddress* into *pduLevel* LSPs,	The redistributed route was being added to the local LSPs.
UPDT: Updating LSP Option Success	IS-IS updated the LSP TLV successfully.
UPDT: Error Adding Summary Reachability in *pduLevel* LSPs	IS-IS failed to add a summary address to the local LSPs.

Table 255 Description on the fields of the debugging isis sending-packet-content command

Field	Description
Sending *pduLevel pduType* on *circuitName*.	IS-IS is sending a PDU. *pduLevel*: L1 or L2. *pduTyp*: PDU type, which can be PSNP or CSNP. *circuitName*: Name of the sending interface.
** **** ** ** ** ** **	Contents in the corresponding CSNP/PSNP packet, including the header, LSP entries, and Authentication Information field.

Table 256 Description on the fields of the debugging isis snp-packet command

Field	Description
CSNP Range from *startLspId* to e*ndLspId*	Range of received CSNP packets *startLspId*: Start LSP ID. e*ndLspId*: End LSP ID.
Rxed *pduType* From *sourceId* (*circuitName*)	PDUs were received. *pduType*: PDU type, which can be PSNP or CSNP. *sourceId*: Source NSAP address of the packet. *circuitName*: Name of the receiving interface.
SNP PDU Dropped	SNP PDU was dropped.
Sending Level *pduLevel* PSNP PDU fails	Sending a PSNP packet failed. *pduLevel*: PDU packet level, which can be L1 or L2.
Sending *content* on *circuitName*	A PSNP packet is being sent. *circuitName*: Name of the sending interface. *content:* PSNP packet content.
SNP not processed, System in Low Memory	System memory was insufficient; therefore, the SNP packets were not processed.
SNP not processed, System in Overload State (Low Memory).	The system is in the Overload state; therefore, the SNP packets were not processed.
Psnp not processed, current IS is Not DIS	The current IS was not a DIS; therefore, the received PSNP packet was not processed.
Csnp not processed on DIS	The CSNP packet was not processed on the DIS.
SNP Authentication Failure	SNP authentication failed.

Table 256 Description on the fields of the debugging isis snp-packet command

Field	Description
Sending *pduLevel* CSNP PDU fails	Sending CSNP packets failed. *pduLevel*: PDU packet level, which can be L1 or L2.
Sending CSNP on P2P Interface *circuitName*	A CSNP packet is being sent through the P2P interface.
Failed to Send CSNP PDU	Sending a CSNP PDU failed.
Sending *content* on *circuitName*	A CSNP PDU is being sent. *circuitName*: Name of the sending interface. *content:* CSNP packet content.

Table 257 Description on the fields of the debugging isis spf-event command

Field	Description
ISIS—*procId*—ISPF—NODE	SPF node-related information *procId*: IS-IS process ID.
ISPF—NODE :(L *sysLevel*)(MT *topoType*) Create NODE *sourceId* Dist: *distanceValue* Nexthops: *nexthopNum* Nbrs: *nbrNum* Parents: *parentNum* [RmtNbr] [Tree]	Root node is created when the direct neighbor relationship is established. *sysLevel*: system level *topoType*: topology type *sourceId*: Source system ID. *distanceValue*: Path cost to the root node *nexthopNum*: Number of nexthops of the node *nbrNum*: Number of neighbors of the node. *parentNum*: Number of parent nodes.
ISPF—NODE :(L *sysLevel*)(MT *topoType*) Create NODE *sourceId* Dist: *distanceValue* Nexthops: *nexthopNum* Nbrs: *nbrNum* Parents: *parentNum* [RmtNbr] [Tree] [Tent] [Direct] [Overload] [Del] [Isolated]	The local interface has become the DIS and SpfNode was created for the pseudonode. sysLevel: system level topoType: topology type sourceId: source system ID. distanceValue: Path cost to the root node nexthopNum: Number of nexthops of the node nbrNum: Number of neighbors of the node. parentNum: Number of parent nodes.
ISPF—NODE :(L *sysLevel*)(MT *topoType*) Adding System *sourceId* [Overload]	The zero fragment of an LSP was received from another system and the SPF node is being created for the system. sysLevel: system level topoType: topology type sourceId: source system ID.
ISPF—NODE :(L *sysLevel*)(MT *topoType*) Create NODE. *sourceId* [Overload]	SPF node is being created. sysLevel: system level topoType: topology type sourceId: source system ID.

Table 257 Description on the fields of the debugging isis spf-event command

Field	Description
ISPF—NODE :(L *sysLevel*)(MT topoType) Create(Exist) NODE. *sourceId* [Overload]	The SPF node was created or the node already exists.
	sysLevel: system level
	topoType: topology type
	sourceId: source system ID.
ISIS—*procId*—ISPF—ADJ	Adjacency-related information
	procId: IS-IS process ID.
ISIS—*procId*—ISPF—LINK	Adjacent link-related information
	procId: IS-IS process ID.
ISPF—ADJ :(L *sysLevel*)(MT *topoType*) Adding P2P ADJ *sourceId*	Adding a point-to-point neighbor
	sysLevel: system level
	topoType: topology type
ISPF—LINK :(L *sysLevel*)(MT topoType) Create(New) LINK *sourceId* --> *destId* OldCost: *oldCost* NewCost: *newCost* [AttAdjs: *attAdjNum*] [Ingore2way] [Tree] [Back] [Incr] [Decr] [Del] [Usage] [Nhop] [Involved] [NewPath]	A P2P link is being created.
	sysLevel: system level
	topoType: topology type
	sourceId: source system ID.
	destId: destination system ID
	oldCost: old path cost value
	newCost: new path cost value
	attAdjNum: Number of ATT neighbors
ISPF—ADJ :(L *sysLevel*)(MT topoType) Adding Bcast ADJ *sourceId*	A broadcast network adjacency is being added
	sysLevel: system level
	topoType: topology type
	sourceId: source system ID.
ISPF—LINK :(L *sysLevel*)(MT topoType) Create(New) LINK *sourceId* --> *destId* OldCost: *oldCost* NewCost: *newCost* [AttAdjs: *attAdjNum*] [Ingore2way] [Tree] [Back] [Incr] [Decr] [Del] [Usage] [Nhop] [Involved] [NewPath]	A broadcast network link is being created.
	sysLevel: system level
	topoType: topology type
	sourceId: source system ID.
	destId: destination system ID
	oldCost: old path cost value
	newCost: new path cost value
	attAdjNum: Number of ATT neighbors
ISIS—*procId*—SPF—EVE	Information about ISPF route calculation
	procId: IS-IS process ID.
SPF—EVE :ISpf starts at *xx:xx:xx*	ISPF route calculation start time
SPF—EVE :Level—*sysLevel*—ISPF Run Started	SPF calculation is started.
	sysLevel: system level
SPF—EVE :Add Self To Tent.	Adding itself to the root node
TENT: Node(SourceId: *sourceId*) is Overload. Ignore its nbrs	The node is overloaded; therefore, its neighbors are ignored.
	sourceId: source system ID.

Table 257 Description on the fields of the debugging isis spf-event command

Field	Description
TENT: New Distance from RootNode(SourceId: *sourceId*) to The Node(SourceId: *sourceId*) is *distanceValue*.	The distance to the root node is updated. sourceId: source system ID.
TENT:Equal cost, add node(SourceId: *sourceId*) to TENT HEAP	The distances from the nodes to the root node are the same. sourceId: source system ID.
ISPF-EVE:Changed Link... *sourceId* --> *destId* OldCost: *oldCost* NewCost: *newCost* [AttAdjs: *attAdjNum*] [Ingore2way] [Tree] [Back] [Incr] [Decr] [Del] [Usage] [Nhop] [Involved] [NewPath]	Changed links. sourceId: source system ID. destId: destination system ID oldCost: old path cost value newCost: new path cost value attAdjNum: Number of ATT neighbors
CHG: Node's usage/nexthop will be changed.Dist: *distanceValue* Nexthops: *nexthopNum* Nbrs: *nbrNum* Parents: *parentNum* [RmtNbr] [Tree] [Tent] [Direct] [Overload] [Del] [Isolated]	The adjacency protocol type or nexthop of the local node is changed. distanceValue: Cost to the root node. nexthopNum: Number of nexthops of the node nbrNum: Number of neighbors of the node. parentNum: Number of parent nodes.
CHG: Ignore2way Link of the ROOT node is considered. Dist: *distanceValue* Nexthops: *nexthopNum* Nbrs: *nbrNum* Parents: *parentNum* [RmtNbr] [Tree] [Tent] [Direct] [Overload] [Del] [Isolated]	For the link of the local node, the two-way check was ignored. distanceValue: Cost to the root node. nexthopNum: Number of nexthops of the node nbrNum: Number of neighbors of the node. parentNum: Number of parent nodes.
ISIS—*procId*—AREA	Area address-related information procId: IS-IS process ID.
AREA:Install one Area [*newareaAddress*] for L *sysLevel* MT *topoType l1referCount / l2referCount* [ADV]	A new area address is added. newareaAddress: New area address sysLevel: system level topoType: topology type l1referCount: Level 1 reference count of the area address. l2referCount: Level 2 reference count of the area address.
AREA:Remove one Area [*oldareaAddress*] for L *sysLevel* MT *topoType l1referCount / l2referCount* [ADV]Remove an area address. oldareaAddress: Old area addresstopoType: topology typel1referCount: Level 1 reference count of t	Remove an area address. oldareaAddress: Old area address topoType: topology type l1referCount: Level 1 reference count of the area address. l2referCount: Level 2 reference count of the area address.
ISIS—*procId*—SPF—PRC	Information about PRC route updates procId: IS-IS process ID.

Table 257 Description on the fields of the debugging isis spf-event command

Field	Description
SPF—PRC:Received L *sysLevel* System Change Event for *msgString*, Change = *chgEvent*	SpfNode change was sent to PRC for processing.
	sysLevel: system level
	msgString: Node change event type.
SPF—PRC:Inform L *sysLevel* Change to Area and Route, Total Change Node:*totalNum*	Inform system ID changes to the area address and route update module
	sysLevel: system level
	totalNum: total node changes
ISIS—*procId*—AREA	Area address-related information and ATT-related information
	procId: IS-IS process ID.
RT Calculation: Elapsed time: *millSeconds* Milliseconds	Route calculation time elapsed in milliseconds
ISIS—*procId*—DEC—PRC	Information of PRC route updates
DEC—PRC :Processing L *sysLevel* LSPs of System : *sourceId*, Change Type = *chgType*	Processing the LSPs of the changed system node.
	sysLevel: system level
	sourceId: source system ID
	chgType: change type

Table 258 Description on the fields of the debugging isis spf-summary command

Field	Description
FWDB-LIMIT::Need to Process ISIS MaxRouteLimit Resume.	Restore the maximum routes in the route table in the case that the route table is not full.

Table 259 Description on the fields of the debugging isis spf-timer command

Field	Description
SPF-TRIG: SPF Scheduled Event (before): *trigEvent*, Run Level: *levelType*.	SPF schedule starts. Triggered event and run level are displayed.
	levelType: Run level of SPF calculation

Table 260 Description on the fields of the debugging isis traffic-eng { advertisement | event } command

Field	Description
Received Extended IS Reach information from LSP	An LSP with the TLV of an extended reachable address was received.
TE: Get TE Info for Circuit %s Failed in Circ Enable.	Tunnel interface has been disabled; therefore, getting tunnel interface information failed.
TE: Add If Te info failed	Adding TE interface information failed.
TE: Rm Traffic Engineering change status to enable.	RM TE status changes to "enabled".
TE: ISIS Update Te LinkInfo In Local TeDb.	ISIS updates TE link information in the local TE database.

Table 261 Description on the fields of the debugging isis update-packet command

Field	Description
pdu length: *pduLen*	Length of received PDU
Adjacency Usage: *adjType*	Adjacency type
Fast Flood *levelType* LSP before SPF	LSPs are fast-flooded before SPF calculation. *levelType*: LSP level, which can be L1 or L2.
RECV: Rxed IS-IS PDU of *pduLen* which is greater than receive size(*receiveLen*)	Received an IS-IS PDU with a *pduLen* greater than receive size (*receiveLen*).
Err!Lsp fragment exceeding Max limit !!!	LSP fragment number exceeds the maximum limit.
UPDT: Circuit up failed	Failed to bring up the interface.
UPDT: Circuit not brought down	Failed to bring down the interface.
Fast Flood L1/L2 LSP when FastFlood timer expired.	Fast-flood L1/L2 LSPs upon expiration of the Fastflood timer.
UPDT: Error! Txmission of Csnp on P2Pckt failed	Transmission of CSNP packets on a P2P network failed.
UPDT: Rx Man area change	The area address in the received LSP changed.
UPDT: Err! Zero Lsp Desc not present	Error! Zero LSP fragment is not present.
UPDT: Err, Match not found for the area addr option	No match is found for the area address in the L1 LSP.
UPDT: Rx att flag change	ATT flag changed in the received LSP.
UPDT: Fatal! Failed to flood Lsp with oload bit set	Failed to flood the LSP because overload bit is set.
UPDT: LSDB Enters Normal Over Load State	The LSDB enters the "overloaded" state.
UPDT: update process recovered from Normal Oload !	The LSDB leaves the "overloaded" state.
UPDT: Rx IP change from config	IP reachable TLV in the received LSP changed.
UPDT: v4/v6 Default Info Origination Denied by Policy.	Default route information failed to pass the policy and therefore was not sent in an LSP.
UPDT: Default Info Origination Permitted by Policy.	Default route information passed the policy and therefore was sent in an LSP.
UPDT: Adj Up failed	Failed to bring up the adjacency.
UPDT: Err1 Processing of Adj down not successful !. SysType *sysLevel* Usage *adjType*	The L1/L2/L12 system failed to process the L1/L2/L12 adjacency down event.
UPDT: Learnt Area Addr change	The area address in the received LSP is changed.
UPDT: MinLspGen Timer hasn't expired. Not generating Lsp	The minimum LSP generation interval has not expired, so no new LSPs can be generated.
UPDT: Err! Unexpected Level *levelType*	The type of the received LSP is invalid. *levelType*: LSP level, L1 or L2
UPDT: Lsp with Invalid IS Nbr Id	The received LSP has an invalid neighbor system ID.
UPDT: Max Area Mismatch.	The maximum area address number in the received LSP does not match that of the current device.
UPDT: Invalid LSP specific hdr !	Invalid received LSP packet header
UPDT: Received LSP Not processed on Broadcast Circuit due to Low Memory, LSP Dropped	The received LSP was dropped due to insufficient memory of the broadcast interface.

Table 261 Description on the fields of the debugging isis update-packet command

Field	Description
UPDT: Received LSP Not processed on P2P Circuit due to Low Memory, Sending Acknowledgement)	The received LSP was dropped due to insufficient memory of the P2P interface and an acknowledgement packet was sent.
UPDT: LSP newer than data base copy.	The received LSP is newer and the local LSDB is updated.
UPDT: Expired Own LSP received. Just Acknowledging.	Remaintime of the received LSP is 0 and therefore only an acknowledge packet is sent.
UPDT: LSP's SeqNumber is 0.	The LSP's sequence number is 0, which is invalid.
UPDT: Err, Area Addr Option in pseudonode Lsps !!	Error: The area address TLV exists in pseudonode LSPs.

Examples # Router A and Router B are interconnected. On Router A, an IS-IS process is created with a System ID of 0000.0000.0001 and router type of **level-1-2**; IS-IS is enabled on VLAN-interface 100 with the IP address 100.1.1.1/24. On Router B, another IS-IS process is created with a System ID of 0000.0000.0002 and router type of **level-1-2**; IS-IS is enabled on VLAN-interface 100 with the IP address 100.1.1.2/24. RTA and RTB are in the same area 49.0001. Enable IS-IS adjacency packet debugging on Router A.

```
<Sysname>debugging isis adjacency
ISIS-1-ADJ: Circuit State Up Success.
ISIS-1-ADJ: Rxed Lan L1 Hello on Vlan100,from SNPA 00e0.fc00.3301.
ISIS-1-ADJ: Sending Lan L1 Hello on Vlan100.
ISIS-1-ADJ: Rxed Lan L2 Hello on Vlan100,from SNPA 00e0.fc00.3301.
ISIS-1-ADJ: Sending Lan L2 Hello on Vlan100.
ISIS-1-ADJ: Rxed Lan L1 Hello on Vlan100,from SNPA 00e0.fc00.3301.
```

// L2 and L2 hello packets were sent and received on VLAN-interface 100, with the SNPA address of the peer as 00e0.fc00.3301.

```
ISIS-1-ADJ: Running DIS Election,Vlan100
ISIS-1-ADJ: Declaring as DIS,DIS Type L2,on Vlan100, Old DIS (null),
 New DIS 0000.0000.0001.01.
ISIS-1-ADJ: Running DIS Election,Vlan100
ISIS-1-ADJ: Declaring as DIS,DIS Type L1,on Vlan100, Old DIS (null),
 New DIS 0000.0000.0001.01.
```

// An *L1/L2 neighbor relationship* w*as established between Router A and Router* B*, and a DIS election was performed.*

VLAN-interface 100 on Router A is connected to VLAN-interface 100 on Router B. An IS-IS process is created on Router A and Router B respectively. Enable interface circuit debugging for IS-IS. Disable IS-IS and then enable it on VLAN-interface 100 of Router A.

```
<Sysname>debugging isis circuit-information
[Sysname]interface vlan-interface 100
[Sysname-Vlan-interface100]undo isis enable
[Sysname-Vlan-interface100]isis enable
ISIS-1-CIRC: Received Circuit OperState ON : Enabling the Circuit
ISIS-1-CIRC: The IP is set to UP for IS-IS on interface Vlan100
```

// The IP address took effect on the IS-IS interface.

Router A and Router B are interconnected and have established an IS-IS adjacency with each other. Router A is elected as the DIS. Enable debugging for the received IS-IS packets on Router A and Router B respectively.

```
ISIS-1-SNP: CSNP Range from 0000.0000.0000.00-00  to  ffff.ffff.ffff.ff-ff.
ISIS-1-SNP: Rxed L1 CSNP From 0000.0000.0001 (Vlan100).
ISIS-1-SNP: CSNP Range from 0000.0000.0000.00-00  to ffff.ffff.ffff.ff-ff.
ISIS-1-SNP: Rxed L2 CSNP From 0000.0000.0001 (Vlan100).
```

// Router B received CSNP packets within a maximum range of 0000.0000.0000.00-00 to ffff.ffff.ffff.ff-ff.

```
ISIS-1-SNP: Sending L1 CSNP on Vlan100.
ISIS-1-SNP: Sending L2 CSNP on Vlan100.
```

// Router B sent CSNP packets.

VLAN-interface 100 on Router A is connected to VLAN-interface 100 on Router B. Create an IS-IS process on Router A and Router B respectively, enable IS-IS on the interfaces, and configure them. On Route A, enable local update debugging; enable IS-IS and then disable it on VLAN-interface 100.

```
<Sysname>debugging isis self-originate-update
[Sysname-Vlan-interface100]undo isis enable
ISIS-1-UPDT: Deleting from the LSP Neighbour option, TLV 2
ISIS-1-UPDT: Circuit Down  Vlan100
ISIS-1-UPDT: Deleting Address 100.1.1.0 from L1 LSPs, TLV: 128
ISIS-1-UPDT: Deleting Address 100.1.1.0 from L2 LSPs, TLV: 128
```

// The *Neighbor TLV was deleted from the local LSPs, and* the *reachable TLV with an IP prefix of 100.1.1.0/24 was deleted from the local L1 and L2 LSPs.*

```
[Sysname-Vlan-interface100] isis enable
ISIS-1-UPDT: Circuit Up Vlan100
ISIS-1-UPDT: Adding Address 100.1.1.0 into L1 LSPs, TLV: 128
ISIS-1-UPDT: Adding Address 100.1.1.0 into L2 LSPs, TLV: 128
ISIS-1-UPDT: Adding in the LSP Neighbour option, TLV 2
```

// The n*eighbor TLV was added to the local LSPs, and the reachable TLV with an IP prefix of 100.1.1.0/24 was added to L1 and L2 LSPs.*

Router A and Router B are interconnected. Enable IS-IS on Router A and Router B respectively. Enable route calculation debugging on Router A.

```
<Sysname>debugging isis spf-event
```

// SPF calculation started, with a system level of L12 and SPF run level of 3.

```
ISIS-1-SPF-TRIG: Starting SPF, Scheduled Event : IS_SPFTRIG_NEWLSP.
Run Level:3
ISIS-1-SPF-EVE: Running Level -1 SPF Run
ISIS-1-SPF-EVE: Adding Self To PATHS
ISIS-1-SPF-EVE: Adding To PATHS:   191.01.01.00/ 255.255.255.00,Cost
 10, Number of next hops 1,  Preference 0
ISIS-1-SPF-EVE: Loading Level-1 Adjacencies
```

```
ISIS-1-SPF-EVE: Processing LSPs of System :0000.0000.0001.00
ISIS-1-SPF-EVE: Updating Level-1 Forwarding table
ISIS-1-SPF-EVE: Level-1 SPF Run Completed
```

// L1 SPF calculation was running and the *L1 IS-IS routing table* was *updated.*

```
ISIS-1-SPF-EVE: Running Level -2 SPF Run
ISIS-1-SPF-EVE: Adding Self To PATHS
ISIS-1-SPF-EVE: Adding To PATHS:   191.01.01.00/ 255.255.255.00,Cost 10, Num
ber of next hops 1,  Preference 0
ISIS-1-SPF-EVE: Loading Level-2 Adjacencies
ISIS-1-SPF-EVE: Adding To PATHS:0000.0000.0001.00,Cost 10, Number of next ho
ps1,  Preference 7
ISIS-1-SPF-EVE: Processing LSPs of System :0000.0000.0001.00
ISIS-1-SPF-EVE: Processing LSPs of Virtual System :0000.0000.0001.00-00
ISIS-1-SPF-EVE: Updating Level-2 Forwarding table
ISIS-1-SPF-EVE: Level-2 SPF Run Completed
ISIS-1-SPF-EVE: Processing the L3 Forward Tables
ISIS-1-SPF-EVE: Beginning Updating the Ipv4 Default Route
ISIS-1-SPF-EVE: no nearest L2IS or local is the nearest L2IS, do NOT generat
e default route!
ISIS-1-SPF-TRIG: Ending SPF Calculation.
ISIS-1-SPF-STAT: SPF Calculation Complete !!!!.
```

// L2 SPF calculation was *running, and IP routing table and default routes* were *updated.*

76 OSPF CONFIGURATION COMMANDS

- *Refer to "MPLS TE Configuration Commands" on page 1565 for OSPF TE related commands.*
- *Refer to "MPLS L2VPN Configuration Commands" on page 1645 and "MPLS L3VPN Configuration Commands" on page 1671.*

abr-summary (OSPF area view)

Syntax **abr-summary** *ip-address* { *mask* | *mask-length* } [**advertise** | **not-advertise**] [**cost** *cost*]

undo abr-summary *ip-address* { *mask* | *mask-length* }

View OSPF area view

Parameters *ip-address*: IP address of the summary route, in dotted decimal format.

mask: Mask of the IP address in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

advertise | **not-advertise**: Advertises or not to advertise the summary route. By default, the summary route is advertised.

cost *cost*: Specifies the cost of the summary route, in the range 1 to 16777215. The default cost is to the biggest cost value among routes that are summarized.

Description Use the **abr-summary** command to configure a summary route on the Area Border Router.

Use the **undo abr-summary** command to remove a summary route.

By default, no route summarization is available on an ABR.

This command is applicable to ABRs only and is used for route summarization in an area. Multiple contiguous networks may be available in an area, where you can summarize them with one network on the ABR for advertisement. The ABR advertises only the summary route to other areas.

With the **undo abr-summary** command used, summarized routes will be advertised.

Examples # Summarize networks 36.42.10.0/24 and 36.42.110.0/24 in Area1 with 36.42.0.0/16 for advertisement to other areas.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 36.42.10.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] network 36.42.110.0 0.0.0.255
[Sysname-ospf-100-area-0.0.0.1] abr-summary 36.42.0.0 255.255.0.0
```

area (OSPF view)

Syntax **area** *area-id*

undo area *area-id*

View OSPF view

Parameters *area-id*: ID of an area, a decimal integer in the range 0 to 4294967295 that is translated into IP address format by the system, or an IP address.

Description Use the **area** command to create an area and enter area view.

Use the **undo area** command to remove a specified area.

No OSPF area is created by default.

Examples # Create Area0 and enter Area 0 view

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0]
```

asbr-summary

Syntax **asbr-summary** *ip-address* { *mask* | *mask-length* } [**tag** *tag* | **not-advertise** | **cost** *cost*]*

undo asbr-summary *ip-address* { *mask* | *mask-length* }

View OSPF view

Parameters *ip-address*: IP address of the summary route in dotted decimal notation.

mask: Summary route mask, in dotted decimal notation.

mask-length: Length of summary route mask, in the range 0 to 32 bits.

not-advertise: Specifies not to advertise the summary route. If the keyword is not specified, the route is advertised.

tag *tag*: Specifies a tag value for the summary route, used by a route policy to control route advertisement, in the range 0 to 4294967295. The value defaults to 1.

cost *cost*: Specifies the cost of the summary route, in the range 1 to 16777214. For Type-1 external routes, the cost defaults to the biggest cost among routes that are summarized. For Type-2 external routes, the cost defaults to the value of the biggest cost among routes that are summarized plus 1.

Description Use the **asbr-summary** command to configure a summary route.

Use the **undo asbr-summary** command to remove a summary route.

No route summarization is configured by default.

With the **asbr-summary** command configured on an ASBR, it summarizes redistributed routes that fall into the specified address range with a single route. If the ASBR resides in an NSSA area, it advertises the summary route in a Type-7 LSA into the area.

With the **asbr-summary** command configured on an NSSA ABR, it summarizes routes in Type-5 LSAs translated from Type-7 LSAs with a single route and advertises the summary route to other areas. This command does not take effect on non NSSA ABRs.

With the **undo asbr-summary** command used, summarized routes will be advertised.

Related commands: **display ospf asbr-summary**.

Examples # Summarize redistributed routes with a single route.

```
<Sysname> system-view
[Sysname] ip route-static 10.2.1.0 24 null 0
[Sysname] ip route-static 10.2.2.0 24 null 0
[Sysname] ospf 100
[Sysname-ospf-100] import-route static
[Sysname-ospf-100] asbr-summary 10.2.0.0 255.255.0.0 tag 2 cost 100
```

authentication-mode

Syntax **authentication-mode** { **simple** | **md5** }

undo authentication-mode

View OSPF area view

Parameters **simple**: Specifies the simple authentication mode.

md5: Specifies the MD5 ciphertext authentication mode.

Description Use the **authentication-mode** command to specify an authentication mode for the OSPF area.

Use the **undo authentication-mode** command to cancel a specified authentication mode.

By default, no authentication mode is configured for an OSPF area.

Routers that reside in the same area must have the same authentication mode: non-authentication, simple, or MD5.

Related commands: **ospf authentication-mode**.

Examples # Specify the MD5 ciphertext authentication mode for OSPF area0.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] authentication-mode md5
```

bandwidth-reference (OSPF view)

Syntax **bandwidth-reference** *value*

undo bandwidth-reference

View OSPF view

Parameters *value*: Specifies a bandwidth reference value for link cost calculation, in the range 1 to 2147483648 Mbps.

Description Use the **bandwidth-reference** command to specify a reference bandwidth value for link cost calculation.

Use the **undo bandwidth-reference** command to restore the default value.

The default value is 100 Mbps.

When links have no cost values configured, OSPF calculates their cost values: Cost=Reference bandwidth value / Link bandwidth. If the calculated cost value is greater than 65535, the maximum cost will be 65535.

Examples # Specify the reference bandwidth value as 1000 Mbps.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] bandwidth-reference 1000
```

default

Syntax **default** { **cost** *cost* | **limit** *limit* | **tag** *tag* | **type** *type* } *

undo default { **cost** | **limit** | **tag** | **type** } *

View OSPF view

Parameters *cost*: Specifies the default cost for redistributed routes, in the range 0 to 16777214.

limit: Specifies the default upper limit of routes redistributed per time, in the range 1 to 2147483647.

tag: Specifies the default tag for redistributed routes, in the range 0 to 4294967295.

type: Specifies the default type for redistributed routes: 1 or 2.

Description Use the **default** command to configure default parameters for redistributed routes: cost, route type (Type1 or Type2), tag, and the upper limit.

Use the **undo default** command to restore default values.

The cost, route type, tag, and the upper limit are 1, 2, 1 and 1000 by default.

Related commands: **import-route (OSPF view)**.

Examples # Configure default parameters cost as 10, upper limit as 20000, tag as 100 and type as 2 for redistributed external routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default cost 10 limit 20000 tag 100 type 2
```

default-cost (OSPF area view)

Syntax **default-cost** *cost*

undo default-cost

View OSPF area view

Parameters *cost*: Specifies a cost for the default route advertised to the Stub or NSSA area, in the range 0 to 16777214.

Description Use the **default-cost** command to specify a cost for the default route advertised to the stub or NSSA area.

Use the **undo default-cost** command to restore the default value.

The cost defaults to 1.

This command is only applicable to the ABR of a stub area or the ABR/ASBR of an NSSA area.

Related commands: **stub (OSPF area view)**, **nssa**.

Examples # Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 20.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
[Sysname-ospf-100-area-0.0.0.1] default-cost 20
```

default-route-advertise (OSPF view)

Syntax **default-route-advertise** [[**always** | **cost** *cost* | **type** *type* | **route-policy** *route-policy-name*] * | **summary cost** *cost*]

default-route-advertise summary cost *cost*

undo default-route-advertise

View OSPF view

Parameters **always**: Generates a default external route in an ASE LSA into the OSPF routing domain, if the router has no default route configured. Without this keyword, the local router can generate a Type-5 LSA describing the default route for advertisement only if the router has the default route configured.

cost *cost*: Specifies the cost for the default route, in the range 0 to 16777214. The default is 1.

type *type*: Specifies the ASE LSA type: 1 or 2, which defaults to 2.

route-policy *route-policy-name*: Specifies the route policy name, a string of 1 to 19 characters. If the default route matches the specified route policy, the route policy affects some value in the ASE LSA.

summary: Advertises the Type-3 summary LSA of the specified default route.

Description Use the **default-route-advertise** command to generate a default route into the OSPF routing domain.

Use the **undo default-route-advertise** command to disable OSPF from distributing a default external route.

By default, no default route is distributed.

Using the **import-route** command cannot redistribute a default route. To do so, use the **default-route-advertise** command. If the default route is not configured on the local router, to generate a Type-5 LSA describing the default route, use the **default-route-advertise always** command.

The **default-route-advertise summary cost** command is applicable only to VPNs, and the default route is redistributed in a Type-3 LSA. The PE router advertises the redistributed default route to the CE router.

Related commands: **import-route (OSPF view)**

Examples # Generate a default route in an ASE LSA into the OSPF routing domain (no default route configured on the router).

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] default-route-advertise always
```

description (OSPF/OSPF area view)

Syntax **description** *description*

undo description

View OSPF view/OSPF area view

Parameters *description*: Describes OSPF process in OSPF view, or describes OSPF area in OSPF area view. *description* is a string of up to 80 characters.

Description Use the **description** command to describe an OSPF process or area.

Use the **undo description** command to remove the description.

No description is configured by default.

Use of this command is only for identification of an OSPF process or area, and has no special meaning.

Examples # Describe the OSPF process 100 as **abc**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] description abc
```

Describe the OSPF area0 as **bone area**.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 0
[Sysname-ospf-100-area-0.0.0.0] description bone area
```

display ospf abr-asbr

Syntax **display ospf** [*process-id*] **abr-asbr**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf abr-asbr** command to display information about ABR/ASBR.

If no process is specified, ABR/ASBR information of all OSPF processes is displayed.

If you use this command on routers in a stub area, no ASBR information is displayed.

Examples # Display information about ABR/ASBR.

```
<Sysname> display ospf abr-asbr

          OSPF Process 1 with Router ID 192.168.1.2
                 Routing Table to ABR and ASBR

Type        Destination       Area        Cost  Nexthop         RtType
 Inter       3.3.3.3           0.0.0.0     3124  10.1.1.2         ASBR
 Intra       2.2.2.2           0.0.0.0     1562  10.1.1.2         ABR
```

Table 262 Description on the fields of the display ospf abr-asbr command

Field	Description
Type	Intra-area router or Inter-area router
Destination	Router ID of an ABR/ASBR
Area	ID of the area of the next hop
Cost	Cost from the router to the ABR/ASBR
Nexthop	Next hop address
RtType	Router type: ABR, ASBR

display ospf asbr-summary

Syntax **display ospf** [*process-id*] **asbr-summary** [*ip-address* { *mask* | *mask-length* }]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

ip-address: Matched IP address, in dotted decimal format.

mask: IP address mask, in dotted decimal format.

mask-length: Mask length, in the range 0 to 32 bits.

Description Use the **display ospf asbr-summary** command to display information about the redistributed routes that are summarized.

If no OSPF process is specified, related information of all OSPF processes is displayed.

If no IP address is specified, information about all summarized redistributed routes will be displayed.

Related commands: **asbr-summary**.

Examples # Display information about all summarized redistributed routes.

```
<Sysname> display ospf asbr-summary

          OSPF Process 1 with Router ID 2.2.2.2
                  Summary Addresses

 Total Summary Address Count: 1

                  Summary Address
 Net          : 30.1.0.0
 Mask         : 255.255.0.0
 Tag          : 20
 Status       : Advertise
 Cost         : 10 (Configured)
 The Count of Route is : 2

 Destination     Net Mask        Proto      Process   Type      Metric
 30.1.2.0        255.255.255.0   OSPF       1         2         1
 30.1.1.0        255.255.255.0   OSPF       1         2         1
```

Table 263 Description on the fields of the display ospf asbr-summary command

Field	Description
Total Summary Address Count	Total summary route number
Net	The address of the summary route
Mask	The mask of the summary route address
Tag	The tag of the summary route
Status	The advertisement status of the summary route
Cost	The cost to the summary route
The Count of Route	The count of routes that are summarized
Destination	Destination address of a summarized route
Net Mask	Network mask of a summarized route
Proto	Routing protocol
Process	Process ID of routing protocol
Type	Type of a summarized route
Metric	Metric of a summarized route

display ospf brief

Syntax **display ospf** [*process-id*] **brief**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf brief** command to display OSPF brief information. If no OSPF process is specified, brief information of all OSPF processes is displayed.

Examples # Display OSPF brief information.

```
<Sysname> display ospf brief
          OSPF Process 1 with Router ID 192.168.1.2
                  OSPF Protocol Information

 RouterID: 192.168.1.2      Border Router:  NSSA
 Route Tag: 0
 Multi-VPN-Instance is not enabled
 Applications Supported: MPLS Traffic-Engineering
 SPF-schedule-interval: 5 0 5000
 LSA generation interval: 5 0 5000
 LSA arrival interval: 1000
 Default ASE Parameter: Metric: 1 Tag: 1 Type: 2
 Route Preference: 10
 ASE Route Preference: 150
 SPF Computation Count: 22
 RFC 1583 Compatible
 Area Count: 1   Nssa Area Count: 1
 ExChange/Loading Neighbors: 0


 Area: 0.0.0.1          (MPLS TE  not enabled)
 Authtype: None Area flag: NSSA
 SPF Scheduled Count: 5
 ExChange/Loading Neighbors: 0

 Interface: 192.168.1.2 (Ethernet1/0)
 Cost: 1       State: DR        Type: Broadcast    MTU: 1500
 Priority: 1
 Designated Router: 192.168.1.2
 Backup Designated Router: 192.168.1.1
 Timers: Hello 10 , Dead 40 , Poll  40 , Retransmit 5 , Transmit Del
ay 1
```

Table 264 Description on the fields of the display ospf brief command

Field	Description
RouterID	Router ID of this router
Border Router	An ABR, ASBR or NSSA ABR
Route Tag	The tag of redistributed routes
Multi-VPN-Instance is not enabled	The current OSPF process supports no multi-VPN-instance
Applications Supported	Applications supported
SPF-schedule-interval	Interval for SPF calculation
LSA generation interval	LSA generation interval
LSA arrival interval	The minimum LSA repeat arrival interval
Default ASE Parameter	Default ASE Parameter: metric, tag, route type.
Route Preference	Internal route priority
ASE Route Preference	External route priority
SPF Computation count	SPF computation count of the OSPF process
RFC1583 Compatible	Compatible with routing rules defined in RFC1583
Area Count	Area number of the current process
Nssa Area Count	NSSA area number of the current process
ExChange/Loading Neighbors	Neighbors in ExChange/Loading state

Table 264 Description on the fields of the display ospf brief command

Field	Description
Area	Area ID in the IP address format
Authtype	Authentication type of the area: Non-authentication, simple authentication, or MD5 authentication
Area flag	The type of the area
SPF scheduled Count	SPF calculation count in the OSPF area
Interface	IP address of the interface
Cost	Interface cost
State	Interface state
Type	Interface network type
MTU	Interface MTU
Priority	Router priority
Designated Router	The Designated Router
Backup Designated Router	The Backup Designated Router
Timers	Intervals of timers: hello, dead, poll, retransmit, and transmit delay
Transmit Delay	LSA transmit delay on the interface

display ospf cumulative

Syntax **display ospf** [*process-id*] **cumulative**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf cumulative** command to display OSPF statistics.

Use of this command is helpful for troubleshooting.

Examples # Display OSPF statistics.

```
<Sysname> display ospf cumulative
          OSPF Process 1 with Router ID 2.2.2.2
                  Cumulations

  IO Statistics
             Type        Input     Output
            Hello           61        122
   DB Description            2          3
   Link-State Req            1          1
Link-State Update            3          3
   Link-State Ack            3          2

  LSAs originated by this router
  Router: 4
  Network: 0
  Sum-Net: 0
```

```
Sum-Asbr: 0
External: 0
NSSA: 0
Opq-Link: 0
Opq-Area: 0
Opq-As: 0

LSAs Originated: 4  LSAs Received: 7

Routing Table:
  Intra Area: 2  Inter Area: 3  ASE/NSSA: 0
```

Table 265 Description on the fields of the display ospf cumulative command

Field	Description
IO statistics	Statistics about inbound/outbound packets and LSAs
Type	OSPF packet type
Input	Packets received
Output	Packets sent
Hello	Hell packet
DB Description	Database Description packet
Link-State Req	Link-State Request packet
Link-State Update	Link-State Update packet
Link-State Ack	Link-State Acknowledge packet
LSAs originated by this router	LSAs originated by this router
Router	Type-1 LSA
Network	Type-2 LSA
Sum-Net	Type-3 LSA
Sum-Asbr	Type-4 LSA
External	Type-5 LSA
NSSA	Type-7 LSA
Opq-Link	Type-9 LSA
Opq-Area	Type-10 LSA
Opq-As	Type-11 LSA
LSA originated	LSA originated
LSA Received	LSA received
Routing Table	Routing table
Intra Area	Intra-area route number
Inter Area	Inter-area route number
ASE/NSSA	Number of ASE/NSSA routes

display ospf error

Syntax **display ospf** [*process-id*] **error**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf error** command to display OSPF error information.

If no process is specified, OSPF error information of all OSPF processes is displayed.

Examples # Display OSPF error information.

```
<Sysname> display ospf error

          OSPF Process 1 with Router ID 192.168.80.100
                  OSPF Packet Error Statistics

0    : OSPF Router ID confusion     0    : OSPF bad packet
0    : OSPF bad version             0    : OSPF bad checksum
0    : OSPF bad area ID             0    : OSPF drop on unnumber interface
0    : OSPF bad virtual link        0    : OSPF bad authentication type
0    : OSPF bad authentication key  0    : OSPF packet too small
0    : OSPF Neighbor state low      0    : OSPF transmit error
0    : OSPF interface down          0    : OSPF unknown neighbor
0    : HELLO: Netmask mismatch      0    : HELLO: Hello timer mismatch
0    : HELLO: Dead timer mismatch   0    : HELLO: Extern option mismatch
0    : HELLO: NBMA neighbor unknown 0    : DD: MTU option mismatch
0    : DD: Unknown LSA type         0    : DD: Extern option mismatch
0    : LS ACK: Bad ack              0    : LS ACK: Unknown LSA type
0    : LS REQ: Empty request        0    : LS REQ: Bad request
0    : LS UPD: LSA checksum bad     0    : LS UPD: Received less recent LSA
0    : LS UPD: Unknown LSA type
```

Table 266 Description on the fields of the display ospf error command

Field	Description
OSPF Router ID confusion	Packets with duplicate route ID
OSPF bad packet	Packets illegal
OSPF bad version	Packets with wrong version
OSPF bad checksum	Packets with wrong checksum
OSPF bad area ID	Packets with invalid area ID
OSPF drop on unnumber interface	Packets dropped on the unnumbered interface
OSPF bad virtual link	Packets on wrong virtual links
OSPF bad authentication type	Packets with invalid authentication type
OSPF bad authentication key	Packets with invalid authentication key
OSPF packet too small	Packets too small in length
OSPF Neighbor state low	Packets received in low neighbor state
OSPF transmit error	Packets with error when being transmitted
OSPF interface down	Shutdown times of the interface
OSPF unknown neighbor	Packets received from unknown neighbors
HELLO: Netmask mismatch	Hello packets with mismatched mask
HELLO: Hello timer mismatch	Hello packets with mismatched hello timer
HELLO: Dead timer mismatch	Hello packets with mismatched dead timer
HELLO: Extern option mismatch	Hello packets with mismatched option field
HELLO: NBMA neighbor unknown	Hello packets received from unknown NBMA neighbors
DD: MTU option mismatch	DD packets with mismatched MTU
DD: Unknown LSA type	DD packets with unknown LSA type
DD: Extern option mismatch	DD packets with mismatched option field
LS ACK: Bad ack	Bad LSAck packets for LSU packets

Table 266 Description on the fields of the display ospf error command

Field	Description
LS ACK: Unknown LSA type	LSAck packets with unknown LSA type
LS REQ: Empty request	LSR packets with no request information
LS REQ: Bad request	Bad LSR packets
LS UPD: LSA checksum bad	LSU packets with wrong LSA checksum
LS UPD: Received less recent LSA	LSU packets without latest LSA
LS UPD: Unknown LSA type	LSU packets with unknown LSA type

display ospf interface

Syntax **display ospf** [*process-id*] **interface** [**all** | *interface-type interface-number*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

all: Display OSPF information of all interfaces.

interface-type interface-number: Interface type and interface number.

Description Use the **display ospf interface** command to display OSPF interface information.

If no OSPF process is specified, OSPF interface information of all OSPF processes is displayed.

Examples # Display OSPF interface information.

```
<Sysname> display ospf interface

          OSPF Process 1 with Router ID 192.168.1.1
                  Interfaces

 Area: 0.0.0.0
 IP Address      Type          State    Cost  Pri   DR              BDR
 192.168.1.1     PTP           P-2-P    1562  1     0.0.0.0         0.0.0.0

 Area: 0.0.0.1
 IP Address      Type          State    Cost  Pri   DR              BDR
 172.16.0.1      Broadcast     DR       1     1     172.16.0.1      0.0.0.0
```

Table 267 Description on the fields of the display ospf interface command

Field	Description
Area	Area ID of the interface
IP address	Interface IP address (regardless of whether TE is enabled or not)
Type	Interface network type: PTP, PTMP, Broadcast, or NBMA
State	Interface state defined by interface state machine: DOWN, Waiting, p-2-p, DR, BDR, or DROther
Cost	Interface cost
Pri	Router priority

Table 267 Description on the fields of the display ospf interface command

Field	Description
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment

display ospf lsdb

Syntax **display ospf** [*process-id*] **lsdb** [**brief** | [{ **ase** | **router** | **network** | **summary** | **asbr** | **nssa** | **opaque-link** | **opaque-area** | **opaque-as** } [*link-state-id*]] [**originate-router** *advertising-router-id* | **self-originate**]]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

brief: Displays brief LSDB information.

ase: Displays Type5 LSA (AS External LSA) information in the LSDB.

router: Displays Type1 LSA (Router LSA) information in the LSDB.

network: Displays Type2 LSA (Network LSA) information in the LSDB.

summary: Displays Type3 LSA (Network Summary LSA) information in the LSDB.

asbr: Displays Type4 LSA (ASBR Summary LSA) information in the LSDB.

nssa: Displays Type7 LSA (NSSA External LSA) information in the LSDB.

opaque-link: Displays Type9 LSA (Opaque-link LSA) information in the LSDB.

opaque-area: Displays Type10 LSA (Opaque-area LSA) information in the LSDB.

opaque-as: Displays Type11 LSA (Opaque-AS LSA) information in the LSDB.

link-state-id: Link state ID, in the IP address format.

originate-router *advertising-router-id*: Specifies the IP address of the router by which to display information of LSAs advertised.

self-originate: Displays information about LSAs originated by this router.

Description Use the **display ospf lsdb** command to display LSDB information.

If no OSPF process is specified, LSDB information of all OSPF processes is displayed.

Examples # Display OSPF LSDB information.

```
<Sysname> display ospf lsdb
         OSPF Process 1 with Router ID 192.168.0.1
                 Link State Database
```

```
                    Area: 0.0.0.0
Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router    192.168.0.2     192.168.0.2        474  36    80000004       0
Router    192.168.0.1     192.168.0.1         21  36    80000009       0
Network   192.168.0.1     192.168.0.1        321  32    80000003       0
Sum-Net   192.168.1.0     192.168.0.1        321  28    80000002       1
Sum-Net   192.168.2.0     192.168.0.2        474  28    80000002       1
                    Area: 0.0.0.1
Type      LinkState ID    AdvRouter          Age  Len   Sequence   Metric
Router    192.168.0.1     192.168.0.1         21  36    80000005       0
Sum-Net   192.168.2.0     192.168.0.1        321  28    80000002       2
Sum-Net   192.168.0.0     192.168.0.1        321  28    80000002       1
```

Table 268 Description on the fields of the display ospf lsdb command

Field	Description
Area	Area
Type	LSA type
LinkState ID	LSA linkstate ID
AdvRouter	The router that advertised the LSA
Age	Aging time of the LSA
Len	Length of the LSA
Sequence	Sequence number of the LSA
Metric	Cost of the LSA

Display Type2 LSA (Network LSA) information in the LSDB.

```
[Sysname] display ospf 1 lsdb network

         OSPF Process 1 with Router ID 192.168.1.1
                     Area: 0.0.0.0
               Link State Database


    Type      : Network
    LS ID     : 192.168.0.2
    Adv Rtr   : 192.168.2.1
    LS Age    : 922
    Len       : 32
    Options   :  E
    Seq#      : 80000003
    Chksum    : 0x8d1b
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.2.1
                          Area: 0.0.0.1
                 Link State Database
    Type      : Network
    LS ID     : 192.168.1.2
    Adv Rtr   : 192.168.1.2
    LS Age    : 782
    Len       : 32
    Options   :  NP
    Seq#      : 80000003
    Chksum    : 0x2a77
    Net Mask  : 255.255.255.0
       Attached Router    192.168.1.1
       Attached Router    192.168.1.2
```

Table 269 Description on the fields of the display ospf 1 lsdb network command

Field	Description
Type	LSA type
LS ID	DR IP address
Adv Rtr	Router that advertised the LSA
LS Age	LSA age time
Len	LSA length
Options	LSA options
Seq#	LSA sequence number
Chksum	LSA checksum
Net Mask	Network mask
Attached Router	ID of the router that established adjacency with the DR, and ID of the DR itself

display ospf nexthop

Syntax **display ospf** [*process-id*] **nexthop**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf nexthop** command to display OSPF next hop information.

If no OSPF process is specified, next hop information of all OSPF processes is displayed.

Examples # Display OSPF next hop information.

```
<Sysname> display ospf nexthop
         OSPF Process 1 with Router ID 192.168.0.1
                 Routing Nexthop Information

  Next Hops:
  Address          Refcount  IntfAddr        Intf Name
 ----------------------------------------------------------------
  192.168.0.1      1         192.168.0.1     Ethernet1/0
  192.168.0.2      1         192.168.0.1     Ethernet1/0
  192.168.1.1      1         192.168.1.1     Ethernet1/1
```

Table 270 Description on the fields of the display ospf nexthop command

Field	Description
Next hops	Information about Next hops
Address	Next hop address
Refcount	Reference count, indicating the number of routes using the nexthop
IntfAddr	Outbound interface address
Intf Name	Outbound interface name

display ospf peer

Syntax **display ospf** [*process-id*] **peer** [**verbose** | [*interface-type interface-number*] [*neighbor-id*]]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

verbose: Displays detailed neighbor information.

interface-type interface-number: Interface type and number

neighbor-id: Neighbor router ID.

Description Use the **display ospf peer** command to display information about OSPF neighbors.

Note that:

If no OSPF process is specified, OSPF neighbor information of all OSPF processes is displayed.

If an interface is specified, the neighbor on the interface is displayed.

If a neighbor ID is specified, detailed information about the neighbor is displayed,

If neither interface nor neighbor ID is specified, brief information about neighbors of the specified OSPF process or all OSPF process is displayed.

Examples # Display detailed OSPF neighbor information.

```
<Sysname> display ospf peer verbose

          OSPF Process 1 with Router ID 1.1.1.1
                  Neighbors
 Area 0.0.0.0 interface 1.1.1.1(Ethernet0/1/0)'s neighbors
 Router ID: 1.1.1.2          Address: 1.1.1.2          GR State: Normal
   State: Full  Mode: Nbr is Master  Priority: 1
   DR: 1.1.1.2  BDR: 1.1.1.1  MTU: 0
   Dead timer due in 33  sec
   Neighbor is up for 02:03:35
   Authentication Sequence: [ 0 ]
   Neighbor state change count: 6
```

Table 271 Description on the fields of the display ospf peer verbose command

Field	Description
Area	Area of the neighbor
Interface	Interface connected to neighbor
Router ID	Neighbor router ID
Address	Neighbor router address
GR State	GR state

Table 271 Description on the fields of the display ospf peer verbose command

Field	Description
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full
Mode	Neighbor mode for DD exchange: Master or Slave
Priority	Router priority
DR	The DR on the interface's network segment
BDR	The BDR on the interface's network segment
MTU	Interface MTU
Dead timer due in 33 sec	Dead timer times out in 33 seconds
Neighbor is up for 93:12:38	The neighbor has been up for 93:12:38
Authentication Sequence	Authentication sequence number
Neighbor state change count	Counts of neighbor state changes

Display brief OSPF neighbor information.

```
<Sysname> display ospf peer

                  OSPF Process 1 with Router ID 1.1.1.1
                       Neighbor Brief Information

 Area: 0.0.0.0
 Router ID       Address         Pri Dead-Time Interface       State
 1.1.1.2         1.1.1.2         1   40        Eth0/1/0        Full/DR
```

Table 272 Description on the fields of the display ospf peer command

Field	Description
Area	Area of neighbors
Router ID	Neighbor router ID
Address	Neighbor interface address
Pri	Router priority
Dead time	Dead interval remained
Interface	The Interface connected to neighbors
State	Neighbor state: Down, Init, Attempt, 2-Way, Exstart, Exchange, Loading or Full

display ospf peer statistics

Syntax **display ospf** [*process-id*] **peer statistics**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf peer statistics** command to display OSPF neighbor statistics.

If no OSPF process is specified, OSPF neighbor statistics of all OSPF processes is displayed.

Examples # Display OSPF neighbor statistics.

```
<Sysname> display ospf peer statistics
                  OSPF Process 1 with Router ID 1.1.1.1
                           Neighbor Statistics

Area ID       Down  Attempt Init 2-Way ExStart Exchange Loading Full Total
0.0.0.1       0      0          0     0     0        0          0        1     1
Total         0      0          0     0     0        0          0        1     1
```

Table 273 Description on the fields of the display ospf peer statistics command

Field	Description
Area ID	Area ID
Down	Under this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Attempt	Available only in an NBMA network, such as Frame Relay, X.25 or ATM. Under this state, the OSPF router has not received any information from a neighbor for a period but can send Hello packets with a longer interval to keep neighbor relationship.
Init	Under this state, the router received a Hello packet from a neighbor but the packet gives no ID of the router, mutual communication is not available.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election finished under this state (or higher).
ExStart	Under this state, the router decides on sequence numbers for DD packets.
Exchange	Under this state, the router exchanges routing information with the neighbor.
Loading	Under this state, the router requests the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

display ospf request-queue

Syntax **display ospf** [*process-id*] **request-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface-type interface-number: Interface type and number.

neighbor-id: Neighbor's router ID.

Description Use the **display ospf request-queue** command to display OSPF request list information.

If no OSPF process is specified, OSPF request list information of all OSPF processes is displayed.

Examples # Display OSPF request list information.

```
<Sysname> display ospf request-queue

         OSPF Process 1 with Router ID 1.1.1.1
                 OSPF Request List

 The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
 Interface 10.1.1.1         Area 0.0.0.0
 Request list:
      Type       LinkState ID      AdvRouter         Sequence   Age
      Router     2.2.2.2           1.1.1.1           80000004   1
      Network    192.168.0.1       1.1.1.1            80000003   1
      Sum-Net    192.168.1.0       1.1.1.1            80000002   2
```

Table 274 Description on the fields of the display ospf request queue command

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Local interface IP address
Area	Area ID
Request list	Request list information
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Router ID of the advertising router
Sequence	LSA sequence number
Age	LSA age time

display ospf retrans-queue

Syntax **display ospf** [*process-id*] **retrans-queue** [*interface-type interface-number*] [*neighbor-id*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface-type interface-number: Specifies an interface.

neighbor-id: Neighbor's router ID.

Description Use the **display ospf retrans-queue** command to display retransmit list information.

If no OSPF process is specified, retransmit list information of all OSPF processes is displayed.

Examples # Display OSPF retransmit list information.

```
<Sysname> display ospf retrans-queue

         OSPF Process 1 with Router ID 1.1.1.1
                 OSPF Retransmit List
```

```
The Router's Neighbor is Router ID 2.2.2.2         Address 10.1.1.2
Interface 10.1.1.1         Area 0.0.0.0
Retransmit list:
     Type       LinkState ID      AdvRouter         Sequence   Age
     Router     2.2.2.2           2.2.2.2           80000004   1
     Network    12.18.0.1         2.2.2.2            80000003   1
     Sum-Net    12.18.1.0         2.2.2.2            80000002   2
```

Table 275 Description on the fields of the display ospf retrans-queue command

Field	Description
The Router's Neighbor is Router ID	Neighbor router ID
Address	Neighbor interface IP address
Interface	Interface address of the router
Area	Area ID
Retrans List	Retransmit list
Type	LSA type
LinkState ID	Link state ID
AdvRouter	Router ID of the advertising router
Sequence	LSA sequence number
Age	LSA age time

display ospf routing

Syntax **display ospf** [*process-id*] **routing** [**interface** *interface-type interface-number*] [**nexthop** *nexthop-address*]

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

interface *interface-type interface-number*: Specifies an interface via which to display routing information advertised.

nexthop *nexthop-address*: Displays routing information with the specified next hop.

Description Use the **display ospf routing** command to display routing table information.

If no OSPF process is specified, routing table information of all OSPF processes is displayed.

Examples # Display OSPF routing table information.

```
<Sysname> display ospf routing

          OSPF Process 1 with Router ID 192.168.1.2
                  Routing Tables

 Routing for Network
 Destination        Cost  Type       NextHop         AdvRouter     Area
 192.168.1.0/24     1562  stub       192.168.1.2     192.168.1.2   0.0.0.0
 172.16.0.0/16      1563  Inter      192.168.1.1     192.168.1.1   0.0.0.0
```

```
Total Nets: 2
Intra Area: 1  Inter Area: 1  ASE: 0  NSSA: 0
```

Table 276 Description on the fields of the display ospf routing command

Field	Description
Destination	Destination network
Cost	Cost to destination
Type	Route type: intra-area, Transit, stub, Inter-area, Type1 External, Type2 External.
NextHop	Next hop address
AdvRouter	Advertising router
Area	Area ID
Total Nets	Total routes
Intra Area	Total intra-area routes
Inter Area	Total inter-area routes
ASE	Total ASE routes
NSSA	Total NSSA routes

display ospf vlink

Syntax **display ospf** [*process-id*] **vlink**

View Any view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf vlink** command to display OSPF virtual link information.

If no OSPF process is specified, the OSPF virtual link information of all OSPF processes is displayed.

Examples # Display OSPF virtual link information.

```
<Sysname> display ospf vlink
          OSPF Process 1 with Router ID 3.3.3.3
                  Virtual Links

 Virtual-link Neighbor-ID  -> 2.2.2.2, Neighbor-State: Full
 Interface: 10.1.2.1 (Serial2/0)
 Cost: 1562  State: P-2-P  Type: Virtual
 Transit Area: 0.0.0.1
 Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 277 Description on the fields of the display ospf vlink command

Field	Description
Virtual-link Neighbor-id	ID of neighbor connected to the router via the virtual link
Neighbor-State	Neighbor State: Down, Attempt, Init, 2-Way, ExStart, Exchange, Loading, Full.
Interface	Local interface's IP address and name of the virtual link

Table 277 Description on the fields of the display ospf vlink command

Field	Description
Cost	Interface route cost
State	Interface state
Type	Type: virtual link
Transit Area	Transit area ID if the interface attached to a virtual link
Timers	Values of timers: Hello, Dead, Poll (NBMA), Retransmit, and Interface transmit delay

enable link-local-signaling

Syntax **enable link-local-signaling**

undo enable link-local-signaling

View OSPF view

Parameters None

Description Use the **enable link-local-signaling** command to enable the OSPF link-local signaling (LLC) capability.

Use the **undo enable link-local-signaling** command to disable the OSPF link-local signaling capability.

By default, this capability is disabled.

Examples # Enable link-local signaling for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
```

enable log

Syntax **enable log** [**config** | **error** | **state**]

undo enable log [**config** | **error** | **state**]

View OSPF view

Parameters **config**: Enables configuration logging.

error: Enables error logging.

state: Enables state logging.

Description Use the **enable** command to enable specified OSPF logging.

Use the **undo enable** command to disable specified logging.

OSPF logging is disabled by default.

If no keyword is specified, all logging is enabled.

Examples # Enable OSPF logging.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable log
```

enable out-of-band-resynchronization

Syntax **enable out-of-band-resynchronization**

undo enable out-of-band-resynchronization

View OSPF view

Parameters None

Description Use the **enable out-of-band-resynchronization** command to enable the OSPF out-of-band resynchronization (OOB-Resynch) capability.

Use the **undo enable out-of-band-resynchronization** command to disable the OSPF out-of-band resynchronization capability.

By default, the capability is disabled.

Examples # Enable the out-of-band resynchronization capability for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
```

filter import/export

Syntax **filter** { *acl-number* | **ip-prefix** *ip-prefix-name* } { **import** | **export** }

undo filter { **import** | **export** }

View OSPF area view

Parameters *acl-number*: ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of up to 19 characters.

import: Filters imported LSAs.

export: Filters exported LSAs.

Description Use the **filter** command to configure exported/imported Summary LSAs filtering on an ABR.

Use the **undo filter** command to disable Summary LSA filtering.

By default, Summary LSAs filtering is disabled.

This command is only available on an ABR.

Examples # Apply IP prefix list **my-prefix-list** to filter inbound Type-3 LSAs, and ACL 2000 to filter outbound Type-3 LSAs in OSPF area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] filter ip-prefix my-prefix-list import
[Sysname-ospf-100-area-0.0.0.1] filter 2000 export
```

filter-policy export (OSPF view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View OSPF view

Parameters *acl-number*: Number of the basic or advanced ACL used to filter routing information by destination address, in the range 2000 to 3999.

ip-prefix-name: Name of the ip-prefix list used to filter routing information by destination address, a string of up to 19 characters.

protocol: Specifies a protocol from which to filter redistributed routes. Protocols include **direct**, **static**, **rip**, **ospf**, **isis** or **bgp**. If no protocol is specified, all redistributed routes are filtered.

process-id: Process ID, which is required when the *protocol* is **rip**, **ospf** or **isis**, in the range 1 to 65535.

Description Use the **filter-policy export** command to configure route redistribution filtering.

Use the **undo filter-policy export** command to disable route redistribution filtering.

By default, route redistribution is disabled.

You can use this command to filter redistributed routes as needed.

Related commands: **import-route (OSPF view)**.

Examples # Filter redistributed routes using ACL 2000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 export
```

filter-policy import (OSPF view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* | **gateway** *ip-prefix-name* } **import**

undo filter-policy import

View OSPF view

Parameters *acl-number*: Number of the basic or advanced ACL used to filter routing information by destination address, in the range 2000 to 3999.

ip-prefix-name: Name of an IP address prefix list used to filter received routes, a string of up to 19 characters.

gateway *ip-prefix-name*: Name of an IP address prefix list used to filter routes received from the specified neighbors, a string of up to 19 characters.

Description Use the **filter-policy import** command to configure the filtering of incoming routes.

Use the **undo filter-policy import** command to disable the filtering.

By default, no filtering of incoming routes is configured.

Examples # Filter received routes using ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 192.168.10.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] ospf 100
[Sysname-ospf-100] filter-policy 2000 import
```

graceful-restart (OSPF view)

Syntax **graceful-restart** [**nonstandard** | **ietf**]

undo graceful-restart

View OSPF view

Parameters **nonstandard**: Enables the non-IETF GR capability.

ietf: Enables the IETF GR capability.

Description Use the **graceful-restart** command to enable the OSPF Graceful Restart capability.

Use the **undo graceful-restart** command to disable the OSPF Graceful Restart capability.

By default, the OSPF Graceful Restart capability is disabled.

Note the following:

- Enable Opaque LSA advertisement and reception with the **opaque-capability enable** command before enabling the IETF GR capability for OSPF.
- Before enabling the non-IETF GR capability for OSPF, enable OSPF LLS (link local signaling) with the **enable link-local-signaling** command and OOB (out of band resynchronization) with the **enable out-of-band-resynchronization** command.
- If the keywords **nonstandard** and **ietf** are not specified when OSPF GR is enabled, **nonstandard** is the default.

Related commands: **enable link-local-signaling**, **enable out-of-band-resynchronization**, **opaque-capability enable**.

Examples # Enable IETF Graceful Restart for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] opaque-capability enable
[Sysname-ospf-1] graceful-restart ietf
```

Enable non-IETF Graceful Restart for OSPF process 1.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] enable link-local-signaling
[Sysname-ospf-1] enable out-of-band-resynchronization
[Sysname-ospf-1] graceful-restart nonstandard
```

graceful-restart help

Syntax **graceful-restart help** { *acl-number* | **prefix** *prefix-list* }

View OSPF view

Parameters *acl-number*: Basic or advanced ACL number, in the range 2000 to 3999.

prefix-list: Name of the specified IP prefix list, a string of 1 to 19 characters.

Description Use the **graceful-restart help** command to configure for which OSPF neighbors the current router can serve as a GR Helper. (The neighbors are specified by the ACL or the IP prefix list.)

By default, the router can serve as a GR Helper for any OSPF neighbor.

Examples # Enable GR Help for OSPF process 1 and configure the router as a GR Helper for OSPF neighbors defined in the ACL 2001.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart help 2001
```

graceful-restart interval (OSPF view)

Syntax **graceful-restart interval** *interval-value*

undo graceful-restart interval

View OSPF view

Parameters *interval-value*: Specifies the Graceful Restart interval, in the range 40 to 1,800 seconds.

Description Use the **graceful-restart interval** command to configure the Graceful Restart interval.

Use the **undo graceful-restart interval** command to restore the default Graceful Restart interval.

By default, the Graceful Restart interval is 120 seconds.

Note that the Graceful Restart interval of OSPF cannot be less than the maximum value of dead intervals on all OSPF interfaces; otherwise, the Graceful Restart of OSPF may fail.

Related commands: **ospf timer dead**.

Examples # Configure the Graceful Restart interval for OSPF process 1 as 100 seconds.

```
<Sysname> system-view
[Sysname] ospf 1
[Sysname-ospf-1] graceful-restart interval 100
```

host-advertise

Syntax **host-advertise** *ip-address cost*

undo host-advertise *ip-address*

View OSPF area view

Parameters *ip-address*: IP address of a host

cost: Cost of the route, in the range 1 to 65535.

Description Use the **host-advertise** command to advertise a host route.

Use the **undo host-advertise** command to remove a host route.

No host route is configured by default.

Examples # Configure host route 1.1.1.1 and specify cost 100 for it.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname] area 0
[Sysname-ospf-100-area-0.0.0.0] host-advertise 1.1.1.1 100
```

import-route (OSPF view)

Syntax **import-route** *protocol* [*process-id* | **allow-ibgp**] [**cost** *cost* | **type** *type* | **tag** *tag* | **route-policy** *route-policy-name*]*

undo import-route *protocol* [*process-id*]

View OSPF view

Parameters *protocol*: Redistributes routes from the specified protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, or **static**.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the *protocol* is **rip**, **ospf**, or **isis**.

allow-ibgp: Allows to redistribute IBGP routes; optional only when the *protocol* is bgp.

cost *cost*: Specifies route cost, in the range 0 to 16777214, which defaults to 1.

type *type*: Specifies cost type, 1 or 2, which defaults to 2.

tag *tag* : Specifies for external LSAs the tag, in the range 0 to 4294967295, which defaults to 1.

route-policy *route-policy-name*: Specifies a route policy to redistribute qualified routes only. *route-policy-name* is a string of up to 19 characters.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable route redistribution from a routing protocol.

No route redistribution is configured by default.

OSPF prioritize routes as follows:

- Intra-area route
- Inter-area route
- Type1 External route
- Type2 External route

An intra-area route is a route in an OSPF area. An inter-area route is between any two OSPF areas. Both of them are internal routes.

An external route is to a destination outside the OSPF AS.

A Type-1 external route is an IGP route, such as RIP or STATIC, which has high reliability and whose cost is comparable with the cost of OSPF internal routes. Therefore, the cost from an OSPF router to a Type-1 external route's destination equals the cost from the router to the corresponding ASBR plus the cost from the ASBR to the external route's destination.

A Type-2 external route is an EGP route, which has low credibility, so OSPF considers the cost from ASBR to a Type-2 external route is much bigger than the cost from the ASBR to an OSPF internal router. Therefore, the cost from an internal router to a Type-2 external route's destination equals the cost from the ASBR to the Type-2 external route's destination.

Related commands: **default-route-advertise (OSPF view)**.

- *The import-route command cannot redistribute **default** routes.*
- *Use the import-route bgp allow-ibgp command with care, because it redistributes both EBGP and IBGP routes that may cause routing loops.*

Examples # Redistribute routes from RIP process 40 and specify the type as type2, tag as 33, and cost as 50 for redistributed routes.

```
<Sysname> system-view
[Sysname> ospf 100
[Sysname-ospf-100] import-route rip 40 type 2 tag 33 cost 50
```

log-peer-change

Syntax **log-peer-change**

undo log-peer-change

View OSPF view

Parameters None

Description Use the **log-peer-change** command to enable the logging of OSPF neighbor state changes.

Use the **undo log-peer-change** command to disable the logging.

The logging is enabled by default.

With this feature enabled, information about neighbor state changes is displayed on the terminal until the feature is disabled.

Examples # Disable the logging of neighbor state changes for OSPF process 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] undo log-peer-change
```

lsa-arrival-interval

Syntax **lsa-arrival-interval** *interval*

undo lsa-arrival-interval

View OSPF view

Parameters *interval*: Specifies the minimum interval between two received identical LSAs in milliseconds, in the range 0 to 60000.

Description Use the **lsa-arrival-interval** command to specify the minimum interval between two identical received LSAs.

Use the **undo lsa-arrival-interval** command to restore the default.

The interval defaults to 1000 milliseconds.

If an LSA that has the same LSA type, LS ID, originating router ID with the previous LSA is received within the interval, the LSA will be discarded. This feature helps you protect routers and bandwidth from being over-consumed due to frequent network changes.

It is recommended the interval set by the **lsa-arrival-interval** command is smaller or equal to the initial interval set by the **lsa-generation-interval** command.

Related commands: **lsa-generation-interval**.

Examples # Set the LSA minimum repeat arrival interval to 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-arrival-interval 200
```

lsa-generation-interval

Syntax **lsa-generation-interval** *maximum-interval* [*initial-interval* [*incremental-interval*]]

undo lsa-generation-interval

View OSPF view

Parameters *maximum-interval*: Maximum LSA generation interval in seconds, in the range 1 to 60.

initial-interval: Minimum LSA generation interval in milliseconds, in the range 10 to 60000. The default is 0 millisecond.

incremental-interval: LSA generation incremental interval in milliseconds, in the range 10 to 60000, which defaults to 5000 milliseconds.

Description Use the **lsa-generation-interval** command to configure the OSPF LSA generation interval.

Use the **undo lsa-generation-interval** command to restore the default.

The LSA generation interval defaults to 5 seconds.

With this command configured, when network changes are not frequent, an LSA is generated at the *initial-interval*. If network changes become frequent, LSA generation interval is incremented by a specified value each time a generation happens, up to the *maximum-interval*.

Related commands: **lsa-arrival-interval**.

Examples # Configure the LSA generation maximum interval as 2 seconds, minimum interval as 100 milliseconds and incremental interval as 100 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsa-generation-interval 2 100 100
```

lsdb-overflow-limit

Syntax **lsdb-overflow-limit** *number*

undo lsdb-overflow-limit

View OSPF view

Parameters *number*: Specifies the upper limit of external LSAs in the LSDB, in the range 1 to 1000000.

Description Use the **lsdb-overflow-limit** command to specify the upper limit of external LSAs in the LSDB.

Use the **undo lsdb-overflow-limit** command to cancel limitation.

External LSAs in the LSDB are unlimited by default.

Examples # Specify the upper limit of external LSAs as 400000.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] lsdb-overflow-limit 400000
```

maximum load-balancing (OSPF view)

Syntax **maximum load-balancing** *maximum*

undo maximum load-balancing

View OSPF view

Parameters *maximum*: Maximum number of load-balanced routes, in the range 1 to 8. A maximum of 1 means no load balancing is enabled.

Description Use the **maximum load-balancing** command to specify the maximum number of load-balanced routes.

Use the **undo maximum load-balancing** command to restore the default.

Examples # Specify the maximum number of load-balanced routes as 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum load-balancing 2
```

maximum-routes

Syntax **maximum-routes** { **external** | **inter** | **intra** } *number*

undo maximum-routes { **external** | **inter** | **intra** }

View OSPF view

Parameters **external**: Specifies the maximum number of external routes.

inter: Specifies the maximum number of inter-area routes.

intra: Specifies the maximum number of intra-area routes.

number: Maximum route number in the range 1 to 10000.

Description Use the **maximum-routes** command to specify the maximum route number of a specified type: inter-area, intra-area, external.

Use the **undo maximum-routes** command to restore the default route maximum value of a specified type.

Examples # Specify the maximum number of intra-area routes as 500.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] maximum-routes intra 500
```

network (OSPF area view)

Syntax **network** *ip-address wildcard-mask*

undo network *ip-address wildcard-mask*

View OSPF area view

Parameters *ip-address*: IP address of a network

wildcard-mask: Wildcard mask of the IP address. For example, the wildcard mask for the subnet mask 255.0.0.0 is 0.255.255.255.

Description Use the **network** command to enable OSPF on the interface attached to the specified network in the area.

Use the **undo network** command to disable OSPF on an interface.

By default, an interface neither belongs to any area nor runs OSPF.

You can configure one or multiple interfaces in an area to run OSPF. Note that the interface's primary IP address must fall into the specified network segment to make the interface run OSPF. If only the interface's secondary IP address falls into the network segment, the interface cannot run OSPF.

Related commands: **ospf**.

Examples # Specify the interface whose primary IP address falls into 131.108.20.0/24 to run OSPF in Area 2.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] network 131.108.20.0 0.0.0.255
```

nssa

Syntax **nssa** [**default-route-advertise** | **no-import-route** | **no-summary**]*

undo nssa

View OSPF area view

Parameters **default-route-advertise**: Usable on an NSSA ABR or an ASBR only. If it is configured on an NSSA ABR, the ABR generates a default route in a Type-7 LSA into the NSSA regardless of whether the default route is available. If it is configured on an ASBR, only a default route is available on the ASBR can it generates the default route in a Type-7 LSA into the attached area.

no-import-route: Usable only on an NSSA ABR that is also the ASBR of the OSPF routing domain to disable redistributing routes in Type7 LSAs into the NSSA area, making sure that routes can be redistributed correctly.

no-summary: Usable only on an NSSA ABR to advertise only a default route in a Type-3 summary LSA into the NSSA area. In this way, all the other summary LSAs are not advertised into the area. Such an area is known as an NSSA totally stub area.

Description Use the **nssa** command to configure the current area as an NSSA area.

Use the **undo nssa** command to restore the default.

By default, no NSSA area is configured.

All routers attached to an NSSA area must be configured with the **nssa** command in area view.

Related commands: **default-cost (OSPF area view)**.

Examples # Configure area1 as an NSSA area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] nssa
```

opaque-capability enable

Syntax **opaque-capability enable**

undo opaque-capability

View OSPF view

Parameters None

Description Use the **opaque-capability enable** command to enable Opaque LSA advertisement and reception. With the command configured, the OSPF device can receive and advertise the Type 9, Type 10 and Type 11 opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

The feature is disabled by default.

Examples # Enable advertising and receiving opaque LSAs.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100]opaque-capability enable
```

ospf

Syntax **ospf** [*process-id* | **router-id** *router-id* | **vpn-instance** *instance-name*]*

undo ospf *process-id*

View System view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

router-id: OSPF router ID, in dotted decimal format.

instance-name: VPN instance name, a string of 1 to 31 case-sensitive characters.

Description Use the **ospf** command to enable an OSPF process.

Use the **undo ospf** command to disable an OSPF process.

No OSPF process is enabled by default.

You can enable multiple OSPF processes on a router and specify different Router IDs for these processes.

When using OSPF as the IGP for MPLS VPN implementation, you need to bind the OSPF process with a VPN instance.

Enabling OSPF first is required before performing other tasks.

Examples # Enable OSPF process 100 and specify Router ID as 10.10.10.1.

```
<Sysname> system-view
[Sysname] ospf 100 router-id 10.10.10.1
[Sysname-ospf-100]
```

ospf authentication-mode

Syntax For MD5/HMAC-MD5 authentication:

ospf authentication-mode { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*

undo ospf authentication-mode { **md5** | **hmac-md5** } *key-id*

For simple authentication:

ospf authentication-mode simple [**plain** | **cipher**] *password*

undo ospf authentication-mode simple

View Interface view

Parameters **md5**: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Authentication key ID, in the range 1 to 255.

plain | cipher : Plain or cipher password. If plain is specified, only plain password is supported and displayed upon displaying the configuration file. If cipher is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. If no keyword is specified, the cipher type is the default for the MD5/HMAC-MD5 authentication mode, and the plain type is the default for the simple authentication mode.

password: Password of plain or cipher. Simple authentication: For plain type password, a plain password is a string of up to 8 characters. For cipher type password, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type password, a plain password is a string of up to 16 characters. For cipher type password, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **ospf authentication-mode** command to set the authentication mode and key ID on an interface.

Use the **undo ospf authentication-mode** command to remove specified configuration.

By default, no authentication is available on an interface.

Interfaces attached to the same network segment must have the same authentication password and mode.

This configuration is not supported on the NULL interface.

Related commands: **authentication-mode**.

Examples # Configure the network 131.119.0.0/16 in area1 to support MD5 cipher authentication, and set the interface key ID to 15, authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
```

```
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode md5
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospf authentication-mode md5 15 cipher abc
```

Configure the network 131.119.0.0/16 in area1 to support simple authentication, and set for the interface the authentication password to **abc**, and password type to cipher.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] network 131.119.0.0 0.0.255.255
[Sysname-ospf-100-area-0.0.0.1] authentication-mode simple
[Sysname-ospf-100-area-0.0.0.1] quit
[Sysname-ospf-100] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospf authentication-mode simple cipher abc
```

ospf cost

Syntax **ospf cost** *value*

undo ospf cost

View Interface view

Parameters *value*: Value of OSPF cost, in the range 1 to 65535.

Description Use the **ospf cost** command to set an OSPF cost for the interface.

Use the **undo ospf cost** command to restore the default OSPF cost for the interface.

By default, an OSPF interface calculates its cost with the formula: interface default OSPF cost=100 Mbps/interface bandwidth(Mbps). Default OSPF costs of some interfaces are:

- 1785 for the 56kbps serial interface
- 1562 for the 64kbps serial interface
- 48 for the E1 (2.048Mbps) interface
- 1 for the Ethernet interface

You can use the **ospf cost** command to set an OSPF cost for an interface manually.

This configuration is not supported on the NULL interface.

Examples # Set the OSPF cost for the interface to 65.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] ospf cost 65
```

ospf dr-priority

Syntax **ospf dr-priority** *priority*

undo ospf dr-priority

View Interface view

Parameters *priority*: DR Priority of the interface, in the range 0 to 255.

Description Use the **ospf dr-priority** command to set the priority for DR/BDR election on an interface.

Use the **undo ospf dr-priority** command to restore the default value.

By default, the priority is 1.

The bigger the value is, the higher the priority.

This configuration is not supported on the NULL interface.

Examples # Set the DR priority on the current interface to 8.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospf dr-priority 8
```

ospf mib-binding

Syntax **ospf mib-binding** *process-id*

undo ospf mib-binding

View System view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **ospf mib-binding** command to bind an OSPF process to MIB operation.

Use the **undo ospf mib-binding** command to restore the default.

By default, MIB operation is bound to the first enabled OSPF process.

Examples # Bind OSPF process 100 to MIB operation.

```
<Sysname> system-view
[Sysname] ospf mib-binding 100
```

Restore the default, that is, bind the first enabled OSPF process to MIB operation

```
<Sysname> system-view
[Sysname] undo ospf mib-binding
```

ospf mtu-enable

Syntax **ospf mtu-enable**

undo ospf mtu-enable

View Interface view

Parameters None

Description Use the **ospf mtu-enable** command to enable an interface to add the real MTU into DD packets.

Use the **undo ospf mtu-enable** command to restore the default.

By default, an interface adds an MTU value of 0 into DD packets, that is, no real MTU is added.

Note that:

- After a virtual link is established via a Virtual-Template or Tunnel, two devices on the link from different vendors may have different MTU values. To make them consistent, set the attached interface's default MTU to 0.
- This configuration is not supported on the NULL interface.

Examples # Enable the interface to add the real MTU value into DD packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospf mtu-enable
```

ospf network-type

Syntax **ospf network-type** { **broadcast** | **nbma** | **p2mp** | **p2p** }

undo ospf network-type

View Interface view

Parameters **broadcast**: Specifies the network type as Broadcast.

nbma: Specifies the network type as NBMA.

p2mp: Specifies the network type as P2MP.

p2p: Specifies the network type as P2P.

Description Use the **ospf network-type** command to set the network type for an OSPF interface.

Use the **undo ospf network-type** command to restore the default network type for an OSPF interface.

By default, the network type of an interface depends on its link layer protocol.

- For Ethernet and FDDI, the default network type is broadcast.
- For ATM, FR, HDLC and X.25, the default network type is NBMA.
- For PPP, LAPB and POS, the default network type is P2P.

Note that:

- If a router on a broadcast network does not support multicast, you can configure the interface's network type as NBMA.
- If an NBMA network is fully meshed, you can configure the network type for interfaces as NBMA. If not, you need to configure the network type as P2MP for two routers having no direct link to exchange routing information through another router.
- When the network type of an interface is NBMA, you need to use the **peer** command to specify a neighbor.
- If only two routers run OSPF on a network segment, you can configure associated interfaces' network type as P2P.

Related commands: **ospf dr-priority**.

This command is not supported on the NULL interface.

Examples # Configure the current interface's network type as NBMA.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] ospf network-type nbma
```

ospf timer dead

Syntax **ospf timer dead** *seconds*

undo ospf timer dead

View Interface view

Parameters *seconds*: Dead interval in seconds, in the range 1 to 2147483647.

Description Use the **ospf timer dead** command to set the dead interval.

Use the **undo ospf timer dead** command to restore the default.

The dead interval defaults to 40s for Broadcast, P2P interfaces and defaults to 120s for P2MP and NBMA interfaces

If an interface receives no hello packet from the neighbor within the dead interval, the interface considers the neighbor down. The dead interval on an interface is at least four times the hello interval. Any two routers attached to the same segment must have the same dead interval.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello**.

Examples # Configure the dead interval on the current interface as 60 seconds.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] ospf timer dead 60
```

ospf timer hello

Syntax **ospf timer hello** *seconds*

undo ospf timer hello

View Interface view

Parameters *seconds*: Hello interval in seconds, in the range 1 to 65535.

Description Use the **ospf timer hello** command to set the hello interval on an interface.

Use the **undo ospf timer hello** command to restore the default hello interval on an interface.

The hello interval defaults to 10s for P2P and Broadcast interfaces, and defaults to 30s for P2MP and NBMA interfaces.

The shorter the hello interval is, the faster the topology converges and the more resources are consumed. Make sure the hello interval on two neighboring interfaces is the same.

This configuration is not supported on the NULL interface.

Related commands: **ospf timer dead**.

Examples # Configure the hello interval on the current interface as 20 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospf timer hello 20
```

ospf timer poll

Syntax **ospf timer poll** *seconds*

undo ospf timer poll

View Interface view

Parameters *seconds*: Poll interval in seconds, in the range 1 to 2147483647.

Description Use the **ospf timer poll** command to set the poll interval on an NBMA interface.

Use the **undo ospf timer poll** command to restore the default value.

By default, the poll interval is 120 seconds.

When an NBMA interface finds its neighbor is dead, it will send hello packets at the poll interval.

Note that:

- The poll interval is at least four times the hello interval.
- This configuration is not supported on the NULL interface.

Related commands: **ospf timer hello**.

Examples # Set the poll timer interval on the current interface to 130 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospf timer poll 130
```

ospf timer retransmit

Syntax **ospf timer retransmit** *interval*

undo ospf timer retransmit

View Interface view

Parameters *interval*: LSA retransmit timer interval in seconds, in the range 1 to 3600.

Description Use the **ospf timer retransmit** command to set the LSA retransmit interval on an interface.

Use the **undo ospf timer retransmit** command to restore the default.

The interval defaults to 5s.

After sending a LSA, an interface waits for an acknowledgement packet. If the interface receives no acknowledgement when the retransmit interval elapses, it will retransmit the LSA.

The retransmit interval should not be so small to avoid unnecessary retransmissions.

This configuration is not supported on the NULL interface.

Examples # Set the LSA retransmit interval to 8 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospf timer retransmit 8
```

ospf trans-delay

Syntax **ospf trans-delay** *seconds*

undo ospf trans-delay

View Interface view

Parameters *seconds*: LSA transmit delay time in seconds, in the range 1 to 3600.

Description Use the **ospf trans-delay** command to set the LSA transmit delay time on an interface.

Use the **undo ospf trans-delay** command to restore the default.

The delay time defaults to 1s.

Each LSA in the LSDB has an age (incremented 1 by a second), but a LSA is not aged out during transmission. It is necessary to add a transmit delay into its age time, which is important for transmission on low speed networks.

This configuration is not supported on the NULL interface.

Examples # Set the LSA transmit delay time to 3 seconds on the current interface.

```
<Sysname> system-view
[Sysname] interface serial2/0
[Sysname-Serial2/0] ospf trans-delay 3
```

peer

Syntax **peer** *ip-address* [**dr-priority** *dr-priority*]

undo peer *ip-address*

View OSPF view

Parameters *ip-address*: Neighbor IP address.

dr-priority: Neighbor DR priority, in the range 0 to 255, the bigger the value, the higher the priority.

Description Use the **peer** command to specify the IP address of an NBMA neighbor, and the DR priority of the neighbor.

Use the **undo peer** command to remove the configuration.

The DR priority of NBMA neighbors defaults to 1.

On an X.25 or Frame Relay network, you can configure mappings to make the network fully meshed (any two routers have a direct link in between), so OSPF can handle DR/BDR election as it does on a broadcast network. However, since routers on the network cannot find neighbors via broadcasting hello packets, you need to specify neighbors and neighbor DR priorities on the routers.

After startup, a router sends a hello packet to neighbors with DR priorities higher than 0. When the DR and BDR are elected, the DR will send hello packets to all neighbors for adjacency establishment.

A router uses the priority set with the **peer** command to determine whether to send a hello packet to the neighbor rather than for DR election. The DR priority set with the **ospf dr-priority** command is used for DR election.

Related commands: **ospf dr-priority**.

Examples # Specify the neighbor IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] peer 1.1.1.1
```

preference

Syntax **preference** [**ase**] [**route-policy** *route-policy-name*] *value*

undo preference [**ase**]

View OSPF view

Parameters **ase**: Sets priority for ASE routes. If the keyword is not specified, using the command sets priority for internal routes.

route-policy: Applies a route policy to set priorities for specified routes.

route-policy-name: Rout policy name, a string of 1 to 19 characters.

value: Priority value, in the range 1 to 255. A smaller value has a higher priority.

Description Use the **preference** command to set the priority of OSPF routes.

Use the **undo preference** command to restore the default.

The priority of OSPF internal routes defaults to 10, and the priority of OSPF external routes defaults to 150.

If a routing policy is specified, priorities defined by the routing policy will apply to matched routes, and the priorities set with the **preference** command apply to OSPF routes not matching the routing policy.

A router may run multiple routing protocols. When several routing protocols find routes to the same destination, the router uses the route found by the protocol with the highest priority.

Examples # Set a priority of 150 for OSPF internal routes.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] preference 150
```

reset ospf counters

Syntax **reset ospf** [*process-id*] **counters** [**neighbor** [*interface-type interface-number*] [*router-id*]]

View User view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

neighbor: Clears neighbor statistics on an interface.

interface-type interface-number: Interface type and interface number.

router-id: Neighbor router ID.

Description Use the **reset ospf counters** command to reset OSPF counters. If no OSPF process is specified, counters of all OSPF processes are reset.

Examples # Clear OSPF counters.

```
<Sysname> reset ospf counters
```

reset ospf process

Syntax **reset ospf** [*process-id*] **process**

View User view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **reset ospf process** command to reset all OSPF processes or a specified process.

Using the **reset ospf process** command will:

- Clear all invalid LSAs without waiting for their timeouts
- Make a newly configured Router ID take effect
- Start a new round of DR/BDR election
- Not remove any previous OSPF configurations

The system prompts whether to reset OSPF process upon execution of this command.

Examples # Reset all OSPF processes.

```
<Sysname> reset ospf process
```

reset ospf redistribution

Syntax **reset ospf** [*process-id*] **redistribution**

View User view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **reset ospf redistribution** command to restart route redistribution.

Examples # Restart route redistribution.

```
<Sysname> reset ospf redistribution
```

rfc1583 compatible

Syntax **rfc1583 compatible**

undo rfc1583 compatible

View OSPF view

Parameters None

Description Use the **rfc1583 compatible** command to make routing rules defined in RFC1583 compatible.

Use the **undo rfc1583 compatible** command to disable the function.

By default, RFC1583 routing rules are compatible.

On selecting the best route when multiple AS external LSAs describe routes to the same destination, RFC1583 and RFC2328 have different routing rules.

Examples # Make RFC1583 routing rules compatible.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] rfc1583 compatible
```

silent-interface (OSPF view)

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View OSPF view

Parameters **all**: Disables all interfaces from sending OSPF packet.

interface-type interface-number: Interface type and interface number.

Description Use the **silent-interface** command to disable specified interfaces from sending any OSPF packet.

Use the **undo silent-interface** command to restore the default.

By default, an interface sends OSPF packets.

A disabled interface is a Passive Interface, which cannot send any Hello packet.

To make no routing information obtained by other routers on a network segment, you can use this command to disable the interface from sending OSPF packets.

Examples # Disable an interface from sending OSPF packets.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] silent-interface serial 2/0
```

snmp-agent trap enable ospf

Syntax **snmp-agent trap enable ospf** [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

undo snmp-agent trap enable ospf [*process-id*] [**ifauthfail** | **ifcfgerror** | **ifrxbadpkt** | **ifstatechange** | **iftxretransmit** | **lsdbapproachoverflow** | **lsdboverflow** | **maxagelsa** | **nbrstatechange** | **originatelsa** | **vifcfgerror** | **virifauthfail** | **virifrxbadpkt** | **virifstatechange** | **viriftxretransmit** | **virnbrstatechange**] *

View System view

Parameters *process-id*: OSPF process ID, in the range 1 to 65535.

ifauthfail: Interface authentication failure information.

ifcfgerror: Interface configuration error information.

ifrxbadpkt: Information about error packets received.

ifstatechange: Interface state change information.

iftxretransmit: Packet receiving and forwarding information.

lsdbapproachoverflow: Information about cases approaching LSDB overflow.

lsdboverflow: LSDB overflow information.

maxagelsa: LSA max age information.

nbrstatechange: Neighbor state change information.

originatelsa: Information about LSAs originated locally.

vifauthfail: Virtual interface authentication failure information.

vifcfgerror: Virtual interface configuration error information.

virifauthfail: Virtual interface authentication failure information.

virifrxbadpkt: Information about error packets received by virtual interfaces.

virifstatechange: Virtual interface state change information.

viriftxretransmit: Virtual interface packet retransmit information.

virnbrstatechange: Virtual interface neighbor state change information.

Description Use the **snmp-agent trap enable ospf** command to enable the sending of SNMP traps for a specified OSPF process. If no process is specified, the feature is enabled for all processes.

Use the **undo snmp-agent trap enable ospf** command to disable the feature.

By default, this feature is enabled.

Refer to "SNMP Configuration Commands" on page 2329 for related information.

Examples # Enable the sending of SNMP traps for all OSPF processes.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable ospf
```

spf-schedule-interval

Syntax **spf-schedule-interval** *maximum-interval* [*minimum-interval* [*incremental-interval*]]

undo spf-schedule-interval

View OSPF view

Parameters *maximum-interval*: Maximum SPF calculation interval in seconds, in the range 1 to 60.

minimum-interval: Minimum SPF calculation interval in milliseconds, in the range 10 to 60000, which defaults to 0.

incremental-interval: Incremental value for increasing SPF calculation interval in milliseconds, in the range 10 to 60000, which defaults to 5000.

Description Use the **spf-schedule-interval** command to set the OSPF SPF calculation interval.

Use the **undo spf-schedule-interval** command to restore the default.

The interval defaults to 5 seconds.

Based on its LSDB, an OSPF router calculates the shortest path tree with itself being the root, and uses it to determine the next hop to a destination. Through adjusting SPF calculation interval, you can protect bandwidth and router resources from being over-consumed due to frequent network changes.

With this command configured, when network changes are not frequent, SPF calculation applies at the *minimum-interval.* If network changes become frequent, the SPF calculation interval is incremented by the *incremental-interval* each time a calculation happens, up to the *maximum-interval*.

Examples # Configure the SPF calculation maximum interval as 10 seconds, minimum interval as 500 milliseconds and incremental interval as 200 milliseconds.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] spf-schedule-interval 10 500 200
```

stub (OSPF area view)

Syntax **stub** [**no-summary**]

undo stub

View OSPF area view

Parameters **no-summary**: Used only on a stub ABR. With it configured, the ABR advertises only a default route in a Summary LSA into the stub area (Such a stub area is known as a totally stub area).

Description Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

No area is a stub area by default.

To cancel the **no-summary** configuration on an ABR, use the **stub** command again to overwirte the previous configuration.

To configure an area as a stub area, all routers attached to it must be configured with this command.

Related commands: **default-cost (OSPF area view)**.

Examples # Configure area1 as a stub area.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] stub
```

stub-router

Syntax **stub-router**

undo stub-router

View OSPF view

Parameters None

Description Use the **stub-router** command to configure the router as a stub router.

Use the **undo stub-router** command to restore the default.

By default, no router is configured as a stub router.

The router LSAs from the stub router may contain different link type values. A value of 3 means a link to the stub network, so the cost of the link remains unchanged. A value of 1, 2 or 4 means a point-to-point link, a link to a transit network or a virtual link; in such cases, a maximum cost value of 65535 is used. Thus, other neighbors find the links to the stub router have such big costs, they will not send packets to the stub router for forwarding as long as there is a route with a smaller cost.

Examples # Enable a stub-router.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] stub-router
```

vlink-peer (OSPF area view)

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **simple** [**plain** | **cipher**] *password* | { **md5** | **hmac-md5** } *key-id* [**plain** | **cipher**] *password*]*

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead** | [**simple** | { **md5** | **hmac-md5** } *key-id*]]*

View OSPF area view

Parameters *router-id*: ID of the neighbor router on the virtual link.

hello *seconds*: Hello interval in seconds, in the range 1 to 8192, which defaults to 10 and is identical to the value on its virtual link neighbor.

retransmit *seconds*: Retransmit interval in seconds, in the range 1 to 3600, which defaults to 5.

trans-delay *seconds*: Transmit delay interval in seconds, in the range 1 to 3600, which defaults to 1.

dead *seconds*: Dead interval in seconds, in the range 1 to 32768, which defaults to 40 and is identical to the value on its virtual link neighbor. The dead interval is at least four times the hello interval.

md5: MD5 authentication.

hmac-md5: HMAC-MD5 authentication.

simple: Simple authentication.

key-id: Key ID for MD5 or HMAC-MD5 authentication, in the range 1 to 255.

plain | **cipher**: Plain or cipher type. If plain is specified, only plain password is supported and displayed upon displaying the configuration file. If cipher is specified, both plain and cipher are supported, but only cipher password is displayed when displaying the configuration file. By default, MD5 and HMAC-MD5 support cipher password, and simple authentication supports plain password.

password: Password of plain or cipher. Simple authentication: For plain type, a plain password is a string of up to 8 characters. For cipher type, a plain password is a string of up to 8 characters, and a cipher password is a string of up to 24 characters. MD5/HMAC-MD5 authentication: For plain type, a plain password is a string of up to 16 characters. For cipher type, a plain password is a string of up to 16 characters, and a cipher password is a string of up to 24 characters.

Description Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

As defined in RFC2328, all non-backbone areas must maintain connectivity to the backbone. You can use the **vlink-peer** command to configure a virtual link to connect an area to the backbone.

Note that:

- The smaller the hello interval is, the faster the network converges and the more network resources are consumed.
- A so small retransmission interval will lead to unnecessary retransmissions. A big value is appropriate for a low speed link.
- You need to specify an appropriate transmission delay with the **trans-delay** keyword.

The authentication mode at the non-backbone virtual link end follows the one at the backbone virtual link end. The two authentication modes (MD5 or Simple) are independent, and you can specify neither of them.

Related commands: **authentication-mode**, **display ospf peer**.

Examples # Configure a virtual link with the neighbor router ID 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 2
[Sysname-ospf-100-area-0.0.0.2] vlink-peer 1.1.1.1
```

77 RIP CONFIGURATION COMMANDS

checkzero

Syntax **checkzero**

undo checkzero

View RIP view

Parameters None

Description Use the **checkzero** command to enable the zero field check on RIP-1 messages.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

After the zero field check is enabled, the router discards RIP-1 messages in which zero fields are non-zero. If all messages are trusty, you can disable this feature to spare the processing time of the CPU.

Examples # Disable the zero field check on RIP-1 messages for RIP process 100.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] undo checkzero
```

default cost (RIP view)

Syntax **default cost** *value*

undo default cost

View RIP view

Parameters *value*: Default metric of redistributed routes, in the range of 0 to 16.

Description Use the **default cost** command to configure the default metric for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

When you use the **import-route** command to redistribute routes from other protocols without specifying a metric, the metric specified by the **default cost** command applies.

Related commands: **import-route (RIP view)**.

Examples # Set the default metric for redistributed routes to 3.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default cost 3
```

default-route originate

Syntax **default-route originate cost** *value*

undo default-route originate

View RIP view

Parameters *value*: Cost of the default route, in the range of 1 to 15.

Description Use the **default-route originate cost** command to advertise a default route with the specified metric to RIP neighbors.

Use the **undo default-route originate** command to disable the sending of a default route.

By default, no default route is sent to RIP neighbors.

The RIP router with this feature configured will not receive any default routes from RIP neighbors.

Examples # Send a default route with a metric of 2.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] default-route originate cost 2
```

Disable default route sending.

```
[Sysname-rip-100] undo default-route originate
```

display rip

Syntax **display rip** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **display rip** command to display the current status and configuration information of the specified RIP process.

- If *process-id* is not specified, information about all configured RIP processes is displayed.
- If *vpn-instance-name* is specified, the RIP configuration of the specified VPN instance is displayed.

Examples # Display the current status and configuration information of all configured RIP processes.

```
<Sysname> display rip
  Public VPN-instance name :

    RIP process : 1
       RIP version : 1
       Preference : 100
       Checkzero : Enabled
       Default-cost : 0
       Summary : Enabled
       Hostroutes : Enabled
       Maximum number of balanced paths : 8
       Update time   :   30 sec(s)  Timeout time         :  180 sec(s)
       Suppress time :  120 sec(s)  Garbage-collect time :  120 sec(s)
       TRIP retransmit time :    5 sec(s)
       TRIP response packets retransmit count :   36
       Silent interfaces : None
       Default routes : Disabled
       Verify-source : Enabled
       Networks :
           192.168.1.0
       Configured peers : None
       Triggered updates sent : 0
       Number of routes changes : 0
       Number of replies to queries : 0
```

Table 278 Description on the fields of the display rip command

Field	Description
Public VPN-instance name (or Private VPN-instance name)	The RIP process runs under a public VPN instance/The RIP process runs under a private VPN instance
RIP process	RIP process number
RIP version	RIP version 1 or 2
Preference	RIP route priority
Checkzero	Indicates whether the zero field check is enabled for RIP-1 messages.
Default-cost	Default cost of the redistributed routes
Summary	Indicates whether the routing summarization is enabled
Hostroutes	Indicates whether to receive host routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIP update interval

Table 278 Description on the fields of the display rip command

Field	Description
Timeout time	RIP timeout time
Suppress time	RIP suppress interval
Garbage-collect time	RIP garbage collection interval
TRIP retransmit time	TRIP retransmit interval for sending update requests and responses
TRIP response packets retransmit count	Maximum retransmit times for update requests and responses
Silent interfaces	Number of silent interfaces, which do not periodically send updates
Default routes	Indicates whether a default route is sent to RIP neighbors
Verify-source	Indicates whether the source IP address is checked on the received RIP routing updates
Networks	Networks enabled with RIP
Configured peers	Configured neighbors
Triggered updates sent	Number of sent triggered updates
Number of routes changes	Number of changed routes in the database
Number of replies to queries	Number of RIP responses

display rip database

Syntax **display rip** *process-id* **database**

View Any view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

Description Use the **display rip database** command to display the active routes in the RIP database, which are sent in normal RIP routing updates.

Examples # Display the active routes in the database of RIP process 100.

```
<Sysname> display rip 100 database
  10.0.0.0/8, cost 1, ClassfulSumm
  10.0.0.0/24, cost 1, nexthop 10.0.0.1, Rip-interface
  11.0.0.0/8, cost 1, ClassfulSumm
  11.0.0.0/24, cost 1, nexthop 10.0.0.1, Imported
```

Table 279 Description on fields of the display rip database command

Field	Description
X.X.X.X/X	Destination address and subnet mask
cost	Cost of the route
classful-summ	Indicates the route is a RIP summary route.
Nexthop	Address of the next hop
Rip-interface	Routes learnt from a RIP-enabled interface
imported	Routes redistributed from other routing protocols

display rip interface

Syntax **display rip** *process-id* **interface** [*interface-type interface-number*]

View Any view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

interface-type interface-number: Specifies an interface.

Description Use the **display rip interface** command to display the RIP interface information of the RIP process.

If no interface is specified, information about all RIP interfaces of the RIP process is displayed.

Examples # Display all the interface information of RIP process 1.

```
<Sysname> display rip 1 interface

 Interface-name: Ethernet1/0
        Address/Mask:1.1.1.1/24                MetricIn/Out:0/1   Version: RIPv1
        Split-horizon/Poison-reverse:on/off     Input/Output:on/on
        Current packets number/Maximum packets number: 234/2000
```

Table 280 Description on the fields of the display rip interface command

Field	Description
Interface-name	The name of an interface running RIP.
Address/Mask	The IP address and Mask of the interface.
MetricIn/Out	Additional routing metric added to the incoming and outgoing routes
Version	RIP version running on the interface
Split-horizon	Indicates whether the split-horizon is enabled (ON: enabled, OFF: disabled).
Poison-reverse	Indicates whether the poison-reverse is enabled (ON: enabled, OFF: disabled)
Input/Output	Indicates if the interface is allowed to receiving (Input) or sending (Output) RIP messages (on is allowed, off is not allowed).
Current packets number/Maximum packets number	Packets to be sent/Maximum packets that can be sent on the interface

display rip route

Syntax **display rip** *process-id* **route** [**statistics** | *ip-address* { *mask* | *mask-length* } | **peer** *ip-address*]

View Any view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

statistics: Displays the route statistics, including total number of routes and number of routes of each neighbor.

ip-address { *mask* | *mask-length* }: Displays route information about a specified IP address.

peer *ip-address*: Displays all routing information learned from a specified neighbor.

Description Use the **display rip route** command to display the routing information of a specified RIP process.

Examples # Display all routing information of RIP process 1.

```
<Sysname> display rip 1 route
 Route Flags: R-RIP, T-TRIP
              P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.23      1         0       RA     102
34.0.0.0/8         21.0.0.23      1         0       RA      23
Peer 21.0.0.12 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.12      1         0       RA      34
12.0.0.0/8         21.0.0.12      1         0       RA      12
```

Display routing information for network 56.0.0.0/8 of RIP process 1.

```
<Sysname> display rip 1 route 56.0.0.0 8
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.23      1         0       RA     102
Peer 21.0.0.12 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.12      1         0       RA      34
```

Display RIP process 1 routing information learned from the specified neighbor.

```
<Sysname> display rip 1 route peer 21.0.0.23
Route Flags: R-RIP, T-TRIP
             P-Permanent, A-Aging, S-Suppressed, G-Garbage-collect
Peer 21.0.0.23 on Ethernet1/0
Destination/Mask    NextHop      Cost     Tag    Flags     Sec
56.0.0.0/8         21.0.0.23      1         0       RA        102
34.0.0.0/8         21.0.0.23      1         0       RA        23
```

Table 281 Description on the fields of the display rip route command

Field	Description
Route Flags	R - RIP route
	T - TRIP route
	P - The route never expires
	A - The route is aging
	S - The route is suppressed
	G - The route is in Garbage-collect state
Peer 21.0.0.23 on Ethernet1/0	Routing information learned on a RIP interface from the specified neighbor
Destination/Mask	Destination IP address and subnet mask
Nexthop	Next hop of the route
Cost	Cost of the route
Tag	Route tag
Flags	Indicates the route state
Sec	Remaining time of the timer corresponding to the route state

Display the routing statistics of RIP process 1.

```
<Sysname> display rip 1 route statistics
Peer         Aging     Permanent    Garbage
21.0.0.23      2           0              3
21.0.0.12      2           0              4
Total          4           0              7
```

Table 282 Description on the fields of the display rip route statistics command

Field	Description
Peer	IP address of a neighbor
Aging	Total number of aging routes learned from the specified neighbor
Permanent	Total number of permanent routes learned from the specified neighbor
Garbage	Total number of routes in the garbage-collection state learned from the specified neighbor
Total	Total number of routes learned from all RIP neighbors

filter-policy export (RIP view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [*protocol* [*process-id*]] [*interface-type interface-number*]

undo filter-policy export [*protocol* [*process-id*]] [*interface-type interface-number*]

View RIP view

Parameters *acl-number*: Number of the Access Control List (ACL) used for filtering outbound routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: Name of the IP prefix list used for filtering outbound routes, a string of 1 to 19 characters.

protocol: Filters outbound routes redistributed from a specified routing protocol, which can be **bgp**, **direct**, **isis**, **ospf**, **rip**, and **static**.

process-id: Process number of the specified routing protocol, in the range of 1 to 65535. You need to specify a process ID when the routing protocol is **rip**, **ospf**, or **isis**.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy export** command to configure RIP to filer advertised routing information.

Use the **undo filter-policy export** command to cancel the filtering of advertised routing information.

By default, RIP does not filter outbound routes.

Note that:

- If *protocol* is specified, RIP filters only the routes redistributed from the specified routing protocol. Otherwise, RIP filters all routes to be advertised.
- If *interface-type interface-number* is specified, RIP filters only the routes advertised by the specified interface. Otherwise, RIP filters routes advertised by all RIP interfaces.

Related commands: **acl** on page 2087, **import-route (RIP view)**, and **ip ip-prefix on page 1210**.

Examples # Reference ACL 2000 to filter outbound routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 export
```

Reference IP prefix list **abc** to filter outbound routes on Ethernet1/0.

```
[Sysname-rip-1] filter-policy ip-prefix abc export static ethernet 1/0
```

filter-policy import (RIP view)

Syntax **filter-policy** { *acl-number* | **gateway** *ip-prefix-name* | **ip-prefix** *ip-prefix-name* [**gateway** *ip-prefix-name*] } **import** [*interface-type interface-number*]

undo filter-policy import [*interface-type interface-number*]

View RIP view

Parameters *acl-number*: Number of the Access Control List (ACL) used for filtering received routes, in the range of 2000 to 3999.

ip-prefix *ip-prefix-name*: References an IP prefix list to filter received routes. The *ip-prefix-name* is a string of 1 to 19 characters.

gateway *ip-prefix-name*: References an IP prefix list to filter routes from the gateway.

interface-type interface-number: Specifies an interface.

Description Use the **filter-policy import** command to configure the filtering of incoming routes.

Use the **undo filter-policy import** command to remove the filtering.

By default, RIP does not filter incoming routes.

Related commands: acl and ip ip-prefix.

Examples # Reference ACL 2000 to filter received routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] filter-policy 2000 import
```

Reference IP prefix list **abc** on Ethernet1/1 to filter all received RIP routes.

```
[Sysname-rip-1] filter-policy ip-prefix abc import ethernet 1/1
```

host-route

Syntax **host-route**

undo host-route

View RIP view

Parameters None

Description Use the **host-route** command to enable host route reception.

Use the **undo host-route** command to disable host route reception.

By default, receiving host routes is enabled.

In some cases, a router may receive many host routes from the same network segment. These routes are not helpful for routing and occupy a large amount of network resources. You can use the **undo host-route** command to disable receiving of host routes.

RIPv2 can be disabled from receiving host routes, but RIPv1 cannot.

Examples # Disable RIP from receiving host routes.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] undo host-route
```

import-route (RIP view)

Syntax **import-route** *protocol* [*process-id*] [**allow-jbgp**] [**cost** *cost* | **route-policy** *route-policy-name* | **tag** *tag*]*

undo import-route *protocol* [*process-id*]

View RIP view

Parameters *protocol*: Specify a routing protocol from which to redistribute routes, currently including **bgp**, **direct**, **isis**, **ospf**, **rip**, **rip** and **static**.

process-id: Process number of the routing protocol, in the range of 1 to 65535, used for **isis**, **rip**, and **ospf**.

cost: Cost for redistributed routes, in the range of 0 to 16. If *cost* is not specified, the default cost specified by the **default cost** command applies.

tag: Tag marking redistributed routes, in the range of 0 to 65,535. The default is 0.

route-policy *route-policy-name*: Specifies a routing policy with 1 to 19 characters.

allow-ibgp: When the *protocol* argument is set to **bgp**, **allow-ibgp** is an optional keyword. The **import-route bgp** command only redistributes EBGP routes, while the **import-route bgp allow-ibgp** command additionally redistributes IBGP routes, which may cause routing loops. Be cautious when using it.

Description Use the **import-route** command to redistribute routes from other routing protocols.

Use the **undo import-route** command to cancel route redistribution.

By default, RIP does not redistribute routes from other routing protocols.

- You can specify a routing policy using keyword **route-policy** to redistribute only the specified routes.
- You can configure a cost for redistributed routes using keyword **cost**.
- You can configure a tag value for redistributed routes using keyword **tag**.

Related commands: **default cost (RIP view)**.

Examples # Redistribute static routes, and set the cost to 4.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] import-route static cost 4
```

Set the default cost for redistributed routes to 3.

```
[Sysname-rip-1] default cost 3
```

Redistribute OSPF routes with the cost being the default cost.

```
[Sysname-rip-1] import-route ospf
```

maximum load-balancing (RIP view)

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View RIP view

Parameters *number*: Maximum number of load balanced routes, in the range 1 to 8.

Description Use the **maximum load-balancing** command to specify the maximum number of load balanced routes.

Use the **undo maximum load-balancing** command to restore the default.

Examples # Specify the maximum number of load balanced routes as 2.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] maximum load-balancing 2
```

network

Syntax **network** *network-address*

undo network *network-address*

View RIP view

Parameters *network-address*: IP address of a network segment, which can be the IP network address of any interface.

Description Use the **network** command to enable RIP on the interface attached to the specified network.

Use the **undo network** command to disable RIP on the interface attached to the specified network.

RIP runs only on the interfaces attached to the specified network. For an interface not on the specified network, RIP neither receives/sends routes on it nor forwards interface route through it. Therefore, you need to specify the network after enabling RIP to validate RIP on a specific interface.

Use the **network** 0.0.0.0 command to enable RIP on all interfaces.

RIP is disabled on an interface by default.

Examples # Enable RIP on the interface attached to the network 129.102.0.0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] network 129.102.0.0
```

peer

Syntax **peer** *ip-address*

undo peer *ip-address*

View RIP view

Parameters *ip-address*: RIP peer IP address, in dotted decimal format.

Description Use the **peer** command to specify a neighbor in the non-broadcast multi-access (NBMA) network. With this command used, routing updates destined to the peer are unicast, rather than multicast or broadcast.

Use the **undo peer** command to remove a neighbor.

By default, no neighbor is specified.

In general, it is not recommended to use the **peer** command, because the neighbor may receive both the unicast and multicast (or broadcast) update of the same route. When you need to use the command, configure the mode of related interface as silent.

Examples # Specify to send unicast updates to peer 202.38.165.1.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] peer 202.38.165.1
```

preference

Syntax **preference** [**route-policy** *route-policy-name*] *value*

undo preference [**route-policy**]

View RIP view

Parameters *route-policy-name*: Routing policy name with 1 to 19 characters.

value: Priority for RIP route, in the range of 1 to 255. The smaller the value, the higher the priority.

Description Use the **preference** command to specify the RIP route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of RIP route is 100.

You can specify a routing policy using keyword **route-policy** to set the specified priority to routes matching the routing policy.

- If a priority is set for matched routes in the routing policy, the priority applies to these routes. The priority of other routes is the one set by the **preference** command.
- If no priority is set for matched routes in the routing policy, the priority of all routes is the one set by the **preference** command.

Examples # Set the RIP route priority to 120.

```
<Sysname> system-view
[Sysname] rip 1
[Sysname-rip-1] preference 120
```

reset rip statistics

Syntax **reset rip** *process-id* **statistics**

View User view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

Description Use the **reset rip statistics** command to clear the statistics of the specified RIP process.

Examples # Clear statistics in RIP process 100.

```
<Sysname> reset rip 100 statistics
```

rip

Syntax **rip** [*process-id*] [**vpn-instance** *vpn-instance-name*]

undo rip [*process-id*] [**vpn-instance** *vpn-instance-name*]

View System view

Parameters *process-id*: RIP process number, in the range of 1 to 65535. The default is 1.

vpn-instance *vpn-instance-name*: Specifies a VPN instance name, a string of 1 to 31 characters.

Description Use the **rip** command to create a RIP process and enter RIP view.

Use the **undo rip** command to disable a RIP process.

By default, no RIP process is enabled.

Note that:

- If no VPN instance is specified, the RIP process will run under public network instance.
- You must create a VPN instance before you apply a RIP process to it. For related configuration, refer to "ip vpn-instance" on page 1696.
- You must create the RIP process before configuring the global parameters. This rule does not apply to interface parameters.
- The configured interface parameters become invalid after you disable the RIP process.

Examples # Create a RIP process and enter rip process view.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1]
```

rip authentication-mode

Syntax **rip authentication-mode** { **md5** { **rfc2082** *key-string key-id* | **rfc2453** *key-string* } | **simple** *password* }

undo rip authentication-mode

View Interface view

Parameters **md5**: MD5 authentication mode.

rfc2453: Uses the message format defined in RFC 2453 (IETF standard).

rfc2082: Uses the message format defined in RFC 2082.

key-id: MD5 key number, in the range of 1 to 255.

key-string: MD5 key string with 1 to 16 characters in plain text format, or 1 to 24 characters in cipher text format. When the **display current-configuration** command is used to display system information, a 24-character cipher string is displayed as the MD5 key string.

simple: Plain text authentication mode.

password: Plain text authentication string with 1 to 16 characters.

Description Use the **rip authentication-mode** command to configure RIP-2 authentication mode and parameters.

Use the **undo rip authentication-mode** command to cancel authentication.

Note that the key string you configured can overwrite the old one if there is any.

Related commands: **rip version**.

With RIPv1, you can configure the authentication mode in interface view. However, the configuration will not take effect because RIPv1 does not support authentication.

Examples # Configure MD5 authentication on Ethernet1/0 with the key string being rose in the format defined in RFC 2453.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] rip version 2
[Sysname-Ethernet1/0] rip authentication-mode md5 rfc2453 rose
```

rip input

Syntax **rip input**

undo rip input

View Interface view

Parameters None

Description Use the **rip input** command to enable the interface to receive RIP messages.

Use the **undo rip input** command to disable the interface from receiving RIP messages.

By default, an interface is enabled to receive RIP messages.

Related commands: **rip output**.

Examples # Enable Ethernet1/0 to receive RIP messages.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip input
```

rip metricin

Syntax **rip metricin** *value*

undo rip metricin

View Interface view

Parameters *value*: Additional metric added to received routes, in the range of 0 to 16.

Description Use the **rip metricin** command to add a metric to the received routes.

Use the **undo rip metricin** command to restore the default.

By default, the additional metric of a received route is 0.

When a valid RIP route is received, the system will add a metric to it and then put it into the routing table. Therefore, the metric of routes received on the configured interface is increased.

Related commands: **rip metricout**.

Examples # Configure an additional metric for routes received on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip metricin 2
```

rip metricout

Syntax **rip metricout** *value*

undo rip metricout

View Interface view

Parameters *value*: Additional metric for outbound routes, in the range of 1 to 16.

Description Use the **rip metricout** command to add a metric to a sent route.

Use the **undo rip metricout** command to restore the default.

By default, the additional metric for sent routes is 1.

Before a RIP route is sent, a metric will be added to it. Therefore, when the metric is configured on an interface, the metric of RIP routes sent on the interface will be increased.

Related commands: **rip metricin**.

Examples # Configure an additional metric of 12 for RIP routes sent on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip metricout 12
```

rip mib-binding

Syntax **rip mib-binding** *process-id*

undo rip mib-binding

View System view

Parameters *process-id*: RIP process number, in the range of 1 to 65535.

Description Use the **rip mib-binding** command to bind MIB operations with a specified RIP process.

Use the **undo rip mib-binding** command to restore the default.

By default, MIB operations are bound to the RIP process with the smallest process ID.

Examples # Configure RIP 100 to accept SNMP requests.

```
<Sysname> system-view
[Sysname] rip mib-binding 100
```

Restore the default.

```
[Sysname] undo rip mib-binding
```

rip output

Syntax **rip output**

undo rip output

View Interface view

Parameters None

Description Use the **rip output** command to enable the interface to send RIP messages.

Use the **undo rip output** command to disable the interface from sending RIP messages.

Sending RIP messages is enabled on an interface by default.

Related commands: **rip input**.

Examples # Enable Serial 2/0 to receive RIP messages.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] rip output
```

rip poison-reverse

Syntax **rip poison-reverse**

undo rip poison-reverse

View Interface view

Parameters None

Description Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples # Enable the poison reverse function for RIP routing updates on Serial 2/0.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] rip poison-reverse
```

rip split-horizon

Syntax **rip split-horizon**

undo rip split-horizon

View Interface view

Parameters None

Description Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

The split horizon function is enabled by default.

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.

- In special cases, make sure it is necessary to disable the split horizon function.
- In Frame Relay, X.25 and other non-broadcast multi-access (NBMA) networks, split horizon should be disabled if multiple VCs are configured on the primary and secondary interfaces to ensure route advertisement. For detailed information, refer to "Frame Relay Configuration Commands" on page 371 and "LAPB and X.25 Configuration Commands" on page 421.

Only the poison reverse function takes effect if both the split horizon and poison reverse functions are enabled.

Examples # Enable the split horizon function on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip split-horizon
```

rip summary-address

Syntax **rip summary-address** *ip-address* { *mask* | *mask-length* }

undo rip summary-address *ip-address* { *mask* | *mask-length* }

View Interface view

Parameters *ip-address*: Summary IP address.

mask: Subnet mask in dotted decimal format.

mask-length: Subnet mask length.

Description Use the **rip summary-address** command to configure RIP-2 to advertise a summary route via the interface.

Use the **undo rip summary-address** command to remove the configuration.

Note that the summary address is valid only when the automatic summarization is disabled.

Related commands: **summary**.

Examples # Advertise a local summary IP address on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip summary-address 10.0.0.0 255.255.255.0
```

rip triggered

Syntax **rip triggered**

undo rip triggered

View Interface view

Parameters None

Description Use the **rip triggered** command to enable triggered RIP.

Use the **undo rip triggered** command to disable triggered RIP.

By default, the triggered RIP is disabled.

Note that triggered RIP can only run on link layer protocols PPP, Frame Relay, and X.25.

Examples # Enable triggered RIP.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] rip triggered
```

rip version

Syntax **rip version** { **1** | **2** [**broadcast** | **multicast**] }

undo rip version

View Interface view

Parameters **1**: RIP version 1.

2: RIP version 2.

broadcast: Sends RIP-2 messages in broadcast mode.

multicast: Sends RIP-2 messages in multicast mode.

Description Use the **rip version** command to specify a RIP version for the interface.

Use the **undo rip version** command to remove the specified RIP version.

By default, no RIP version is configured for an interface, which uses the global RIP version. If the global RIP version is not configured, the interface can only send RIP-1 broadcasts and can receive RIP-1 broadcasts and unicasts, and RIP-2 broadcasts, multicasts and unicasts.

If RIP-2 is specified with no sending mode configured, RIP-2 messages will be sent in multicast mode.

When RIP-1 runs on an interface, the interface will:

- Send RIP-1 broadcast messages
- Receive RIP-1 broadcast messages
- Receive RIP-1 unicast messages

When RIP-2 runs on the interface in broadcast mode, the interface will:

- Send RIP-2 broadcast messages
- Receive RIP-1 broadcast messages
- Receive RIP-1 unicast messages
- Receive RIP-2 broadcast messages
- Receive RIP-2 multicast messages
- Receive RIP-2 unicast messages

When RIP-2 runs on the interface in multicast mode, the interface will:

- Send RIP-2 multicast messages
- Receive RIP-2 broadcast messages
- Receive RIP-2 multicast messages
- Receive RIP-2 unicast messages

Examples # Configure Ethernet1/0 to broadcast RIP-2 messages.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] rip version 2 broadcast
```

silent-interface (RIP view)

Syntax **silent-interface** { **all** | *interface-type interface-number* }

undo silent-interface { **all** | *interface-type interface-number* }

View RIP view

Parameters **all**: Silents all interfaces.

interface-type interface-number: Specifies an interface.

Description Use the **silent-interface** command to disable an interface or all interfaces from sending routing updates. That is, the interface only receives but does not send RIP messages.

Use the **undo silent-interface** command to restore the default.

By default, all interfaces are allowed to send routing updates.

Examples # Configure all interfaces to work in the silent mode, and then activate Ethernet1/0.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] silent-interface all
[Sysname-rip-100] undo silent-interface ethernet1/0
[Sysname-rip-100] network 131.108.0.0
```

summary

Syntax **summary**

undo summary

View RIP view

Parameters None

Description Use the **summary** command to enable automatic RIP-2 summarization. Natural masks are used to advertise summary routes so as to reduce the size of routing tables.

Use the **undo summary** command to disable automatic RIP-2 summarization so that all subnet routes can be broadcasted.

By default, automatic RIP-2 summarization is enabled.

Enabling automatic RIP-2 summarization can reduce the size of the routing table to enhance the scalability and efficiency of large networks.

Related commands: **rip version**.

Examples # Enable RIP-2 automatic summarization.

```
<Sysname> system-view
[Sysname] rip
[Sysname-rip-1] summary
```

timers

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** } *

View RIP view

Parameters *garbage-collect-value*: Garbage-collect timer time in seconds, in the range of 1 to 3600.

suppress-value: Suppress timer time in seconds, in the range of 0 to 3600.

timeout-value: Timeout timer time in seconds, in the range of 1 to 3,600.

update-value: Update timer time in seconds, in the range of 1 to 3,600.

Description Use the **timers** command to configure RIP timers. By adjusting RIP timers, you can improve network performance.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIP is controlled by the above four timers.

- The update timer defines the interval between routing updates.
- The timeout timer defines the route aging time. If no routing update related to a route is received after the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIP route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the Garbage-Collect timer length, RIP advertises the route with the routing metric set to 16. If no routing update is announced for that route after the Garbage-Collect timer expires, the route will be deleted from the routing table.

Note that:

- Generally, you are not recommended to change the default values of these timers.
- The time lengths of these timers must be kept consistent on all routers and access servers in the network.

Examples # Specifies the update, timeout, suppress, and garbage-collect timers as 5, 15, 15 and 30 respectively.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] timers update 5
[Sysname-rip-100] timers timeout 15
[Sysname-rip-100] timers suppress 15
[Sysname-rip-100] timers garbage-collect 30
```

trip retransmit count

Syntax **trip retransmit count** *retransmit-count-value*

undo trip retransmit count

View RIP view

Parameters *retransmit-count-value:* Upper limit for retransmitting an Update Request or Update Response, in the range 1 to 3600.

Description Use the **trip retransmit count** command to configure the upper limit for retransmitting an Update Request or Update Response.

Use the **undo validate-source-address** command to restore the default.

The default upper limit is 36.

Examples # Configure an upper limit of 20 for retransmitting an Update Request or Update Response.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] trip retransmit count 20
```

trip retransmit timer

Syntax **trip retransmit timer** *retransmit-time-value*

undo trip retransmit timer

View RIP view

Parameters *retransmit-time-value:* Interval in seconds for retransmitting an Update Request or Update Response, in the range 1 to 3600.

Description Use the **trip retransmit timer** command to configure the interval for retransmitting an Update Request or Update Response.

Use the **undo validate-source-address** command to restore the default.

The default interval is 5 seconds.

For two routers on an analog dial-up link, the difference between retransmission intervals on the two ends must be bigger than 50 seconds; otherwise, they can not become TRIP neighbors.

Examples # Configure an interval of 80 seconds for retransmitting an Update Request or Update Response.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] trip retransmit timer 80
```

validate-source-address

Syntax **validate-source-address**

undo validate-source-address

View RIP view

Parameters None

Description Use the **validate-source-address** command to enable the source IP address validation on incoming RIP routing updates.

Use the **undo validate-source-address** command to disable the source IP address validation.

The source IP address validation is enabled by default.

Generally, disabling the validation is not recommended.

Examples # Enable the source IP address validation on incoming messages.

```
<Sysname> system-view
[Sysname-rip] rip 100
[Sysname-rip-100] validate-source-address
```

version

Syntax **version** { **1** | **2** }

undo version

View RIP view

Parameters **1**: Specifies the RIP version as RIP-1.

2: Specifies the RIP version as RIP-2. RIP-2 messages are multicast.

Description Use the **version** command to specify a global RIP version.

Use the **undo version** command to remove the configured global RIP version.

By default, the global RIP version is RIP-1.

Note that:

- If an interface has an RIP version specified, the RIP version takes precedence over the global one.

- If no RIP version is specified for the interface and the global version is RIP-1, the interface inherits RIP-1, and then it can send RIP-1 broadcasts, and receive RIP-1 broadcasts and unicasts.
- If no RIP version is specified for the interface and the global version is RIP-2, the interface inherits RIP-2, and then it can send RIP-2 multicasts, and receive RIP-2 broadcasts, multicasts and unicasts.
- On a ComwareV5 device, you can configure the RIP version in RIP view and in interface view. On a ComwareV3 device, you can only perform such configuration in interface view.
- To enable a ComwareV5 device in the RIP-1 mode to interoperate with a ComwareV3 device in the RIP-2 broadcast mode, you need to use the **undo version** command in RIP view and the **undo rip version** in interface view to remove related RIP version configuration from the ComwareV5 device.
- For a ComwareV5 device, the case that no RIP version is configured is different from the case that RIP-1 is configured. The former one uses the default RIP-1 version that is compatible with RIP-2, but the latter one is not compatible with RIP-2.

Examples # Specify RIP-2 as the global RIP version.

```
<Sysname> system-view
[Sysname] rip 100
[Sysname-rip-100] version 2
```

78 ROUTING POLICY COMMON CONFIGURATION COMMANDS

Routing policy common configuration commands are applicable to both IPv4 and IPv6.

apply as-path

Syntax **apply as-path** *as-number*&<1-10> [**replace**]

undo apply as-path

View Routing policy view

Parameters *as-number*: Autonomous system number, in the range of 1 to 65535.

&<1-10>: Indicates you can enter *as-number* up to 10 times.

replace: Replaces the original AS number.

Description Use the **apply as-path** command to apply the specified AS numbers to BGP routes.

Use the **undo apply as-path** command to remove the clause configuration.

No AS_PATH attribute is set by default.

With the **replace** keyword, using the **apply as-path** command replaces the original AS_PATH attribute with specified AS numbers. Without the **replace** keyword, using this command adds the specified AS numbers before the original AS_PATH attribute.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, add AS number 200 before the original AS_PATH attribute.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply as-path 200
```

apply comm-list delete

Syntax **apply comm-list** *comm-list-number* **delete**

undo apply comm-list

View Routing policy view

Parameters *comm-list-number*: Community list number. The basic community list number ranges from 1 to 99. The advanced community list number ranges from 100 to 199.

Description Use the **apply comm-list delete** command to remove community attributes in BGP routing information specified by the community list.

Use the **undo apply comm-list** command to remove the clause configuration.

No community attributes are removed by default.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If BGP routing information matches AS-path-ACL 1, remove community attributes specified in community list 1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply comm-list 1 delete
```

apply community

Syntax **apply community** { **none** | **additive** | { *community-number*&<1-16> | *aa:nn*&<1-16> | **internet** | **no-export-subconfed** | **no-export** | **no-advertise** } ***** [**additive**] }

undo apply community

View Routing policy view

Parameters **none**: Removes community attributes of BGP routes.

community-number: Community sequence number, in the range 1 to 4294967295.

aa:nn: Community number; both aa and nn are in the range 0 to 65535.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

internet: Sets the **internet** community attribute for matched BGP routes. Routes with this attribute are advertised to all BGP peers.

no-export-subconfed: Sets the **no-export-subconfed** community attribute for matched BGP routes. Routes with this attribute are not advertised out the sub autonomous system.

no-advertise: Sets the **no-advertise** community attribute for matched BGP routes. Routes with this attribute are not advertised to any peers.

no-export: Sets the **no-export** community attribute for matched BGP routes. Routes with this attribute are not advertised out the autonomous system or confederation, but can be advertised to other sub ASs in the confederation.

additive: Adds the specified community attributes to the original community attribute of a matched BGP route.

Description Use the **apply community** command to set the specified community attribute for BGP routes.

Use the **undo apply community** command to remove the apply clause.

No community attribute is set by default.

Related commands: **ip community-list**, **if-match community**, **route-policy**.

Examples # Create routing policy **setcommunity** with node 16 and matching mode as permit. Set the no-export community attribute for BGP routes passing AS-path-ACL 8.

```
<Sysname> system-view
[Sysname] route-policy setcommunity permit node 16
[Sysname-route-policy] if-match as-path 8
[Sysname-route-policy] apply community no-export
```

apply cost

Syntax **apply cost** [+ | -] *value*

undo apply cost

View Routing policy view

Parameters **+**: Increases cost value.

+: Decreases cost value.

cost: Specifies a cost from 0 to 4294967295.

Description Use the **apply cost** command to set a cost for routing information.

Use the **undo apply cost** command to remove the clause configuration.

No cost is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches the outbound interface Serial 2/0, set the cost for the route to 120.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface serial 2/0
[Sysname-route-policy] apply cost 120
```

apply cost-type

Syntax **apply cost-type** { **external** | **internal** | **type-1** | **type-2** }

undo apply cost-type

View Routing policy view

Parameters **external**: IS-IS external route.

internal: IS-IS internal route.

type-1: Type-1 external route of OSPF.

type-2: Type-2 external route of OSPF.

Description Use the **apply cost-type** command to set a cost type for routing information.

Use the **undo apply cost-type** command to remove the clause configuration.

No cost type is set for routing information by default.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches tag 8, set the cost type for the route to IS-IS internal route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply cost-type internal
```

apply extcommunity

Syntax **apply extcommunity** { **rt** *route-target* }&<1-16> [**additive**]

undo apply extcommunity

View Routing policy view

Parameters **rt** *route-target*: Sets the route target extended community attribute, which is a string of 3 to 21 characters. *route-target* has two forms:

16-bit AS number: 32-bit self-defined number, for example, 101:3;

32-bit IP address: 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

additive: Adds to the original community attribute of a route.

Description Use the **apply extcommunity** command to apply the specified extended community attribute to BGP routes.

Use the **undo apply extcommunity** command to remove the clause configuration.

No extended community attribute is set for routing information by default.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, add the RT extended community attribute 100:2 to the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply extcommunity rt 100:2 additive
```

apply isis

apply isis { **level-1** | **level-1-2** | **level-2** }

undo apply isis

View Routing policy view

Parameters **level-1**: Redistributes routes into IS-IS level-1 area.

level-2: Redistributes routes into IS-IS level-2 area.

level-1-2: Redistributes routes into IS-IS level-1 and level-2 areas.

Description Use the **apply isis** command to redistribute routes into a specified ISIS level.

Use the **undo apply isis** command to remove the clause configuration.

No level is set by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches tag 8, redistribute the route to IS-IS level-2 area.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
[Sysname-route-policy] apply isis level-2
```

apply local-preference

Syntax **apply local-preference** *preference*

undo apply local-preference

View Routing policy view

Parameters *preference*: BGP local preference, in the range 0 to 4294967295.

Description Use the **apply local-preference** command to apply the specified local preference to BGP routes.

Use the **undo apply local-preference** command to remove the clause configuration.

No local preference is set for BGP routing information by default.

Related commands: **route-policy**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the local preference for the route to 130.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply local-preference 130
```

apply mpls-label

Syntax **apply mpls-label**

undo apply mpls-label

View Routing policy view

Parameters None

Description Use the **apply mpls-label** command to set MPLS label for routing information.

Use the **undo apply mpls-label** command to remove the clause configuration.

No MPLS label is set by default.

If MPLS label failed to apply, the routing information can not be advertised.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set MPLS label for the route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply mpls-label
```

apply origin

Syntax **apply origin** { **igp** | **egp** *as-number* | **incomplete** }

undo apply origin

View Routing policy view

Parameters **igp**: Sets the origin of BGP routing information to IGP.

egp: Sets the origin of BGP routing information to EGP.

as-number: Autonomous system number for EGP routes, in the range of 1 to 65535.

incomplete: Sets the origin of BGP routing information to unknown.

Description Use the **apply origin** command to apply the specified origin attribute to BGP routes.

Use the **undo apply origin** command to remove the clause configuration.

No origin attribute is set for routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost** and **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches AS-path-ACL 1, set the origin for the route to IGP.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply origin igp
```

apply preference

Syntax **apply preference** *preference*

undo apply preference

View Routing policy view

Parameters *preference*: Routing preference, in the range of 1 to 255.

Description Use the **apply preference** command to set a preference for a routing protocol.

Use the **undo apply preference** command to remove the clause configuration.

No preference is set for a routing protocol by default.

If you set preferences for routing protocols with the **preference** command, using the **apply preference** command will set a new preference for a matched routing protocol. Other routing protocols not satisfying criteria still use the preferences set by the **preference** command.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches OSPF external route type, set the preference for the routing protocol to 90.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1or2
[Sysname-route-policy] apply preference 90
```

apply preferred-value

Syntax **apply preferred-value** *preferred-value*

undo apply preferred-value

View Routing policy view

Parameters *preferred-value*: Preferred value, in the range of 0 to 65535.

Description Use the **apply preferred-value** command to apply a preferred value to BGP routes.

Use the **undo apply preferred-value** command to remove the clause configuration.

No preferred value is set for BGP routes by default.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a BGP route matches AS-path-ACL 1, set the preferred value 66 for the BGP route.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply preferred-value 66
```

apply tag

Syntax **apply tag** *value*

undo apply tag

View Routing policy view

Parameters *value*: Tag value, in the range 0 to 4294967295.

Description Use the **apply tag** command to set a specified tag value for RIP, OSPF or IS-IS routing information.

Use the **undo apply tag** command to remove the clause configuration.

No routing tag is set for RIP, OSPF or IS-IS routing information by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply local-preference**, **apply cost** and **apply origin**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. If a route matches OSPF external route type 1, set the tag of the route to 100.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type external-type1
[Sysname-route-policy] apply tag 100
```

display ip as-path

Syntax **display ip as-path** [*as-path-acl number*]

View Any view

Parameters *as-path-acl-number*: AS path ACL number, in the range of 1 to 256.

Description Use the **display ip as-path** command to display BGP AS path ACL information.

Information about all BGP AS path ACLs will be displayed if no *as-path-acl-number* is specified.

Related commands: **ip as-path**, **if-match as-path** and **apply as-path**.

Examples # Display the information of BGP AS path ACL 1.

```
<Sysname> display ip as-path-acl 1
ListID    Mode      Expression
1         permit    2
```

Table 283 Description on the fields of the display ip as-path-acl command

Field	Description
ListID	AS path ACL ID
Mode	Matching mode: permit, deny
Expression	Regular expression for matching

display ip community-list

Syntax **display ip community-list** [*basic-community-list-number* | *adv-community-list-number*]

View Any view

Parameters *basic-community-list-number*: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

Description Use the **display ip community-list** command to display BGP community list information.

All BGP community list information will be displayed if no *basic-community-list-number* or *adv-community-list-number* is specified.

Related commands: **ip community-list**, **if-match community** and **apply community**.

Examples # Display the information of the BGP community list 1.

```
<Sysname> display ip community-list 1
Community List Number 1
         permit  1:1 1:2 2:2
```

display ip extcommunity-list

Syntax **display ip extcommunity-list** [*ext-comm-list-number*]

View Any view

Parameters *ext-comm-list-number*: Extended community list number, in the range of 1 to 199.

Description Use the **display ip extcommunity-list** command to display BGP extended community list information.

All BGP extended community list information will be displayed if no *ext-comm-list-number* is specified.

Related commands: **ip extcommunity-list**, **if-match extcommunity**, **apply extcommunity**.

Examples # Display the information of BGP extended community list 1.

```
<Sysname> display ip extcommunity-list 1
Extended Community List Number 1
         permit rt : 9:6
```

display route-policy

Syntax **display route-policy** [*route-policy-name*]

View Any view

Parameters *route-policy-name*: Routing policy name, a string of 1 to 19 characters.

Description Use the **display route-policy** command to display routing policy information.

All routing policy information will be displayed if no *route-policy-name* is specified.

Related commands: **route-policy**.

Examples # Display the information of routing policy 1.

```
<Sysname> display route-policy policy1
Route-policy : policy1
  permit : 10
        if-match ip-prefix abc
        apply cost 120
```

Table 284 Description on the fields of the display route-policy command.

Field	Description
Route-policy	Routing policy name
Permit	permit mode: permit, deny
if-match ip-prefix abc	Match criterion
apply cost 120	If the match criterion is satisfied, set the route cost to 120.

if-match as-path

Syntax **if-match as-path** *as-path-number*&<1-16>

undo if-match as-path [*as-path-number*&<1-16>]

View Routing policy view

Parameters *as-path-number*: AS path ACL number, in the range of 1 to 256.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match as-path** command to specify AS path ACL(s) for matching against the AS path attribute of BGP routing information.

Use the **undo if-match as-path** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of a route policy, used for filtering BGP routing information and specifying match criteria according to the AS path attribute of routing information.

Related commands: **route-policy**, **ip as-path** *acl*.

Examples # Define as-path-acl 2, allowing routing information containing AS 200 or 300 to pass. Define routing policy **test** with node 10, and set an if-match clause using the as-path-acl for matching.

```
<Sysname> system-view
[Sysname] ip as-path 2 permit _*200.*300
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match as-path 2
```

if-match community

Syntax **if-match community** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

undo if-match community [*basic-community-list-number* | *adv-community-list-number*]&<1-16>

View Routing policy view

Parameters *basic-community-list-number*: Basic community list number, in the range of 1 to 99.

adv-community-list-number: Advanced community list number, in the range of 100 to 199.

whole-match: Specifies the exact match. All and only the specified communities must be present.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match community** command to specify community list(s) for matching against the community attribute of BGP routing information.

Use the **undo if-match community** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of route policy, used for filtering BGP routing information and specifying match criterion according to the community attribute of BGP routing information.

Related commands: **route-policy** and **ip community-list**.

Examples # Define community-list 1, allowing routing information with community number 100 or 200 to pass. Then define a routing policy named test, whose node 10 is defined with an if-match clause to reference the community-list for matching.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit 100 200
[Sysname] route-policy test permit node 10
[Sysname-route-policy] if-match community 1
```

if-match cost

Syntax **if-match cost** *value*

undo if-match cost

View Routing policy view

Parameters *cost*: Specifies the cost to match, ranging from 0 to 4294967295.

Description Use the **if-match cost** command to specify a cost for matching against the cost of a route.

Use the **undo if-match cost** command to remove the match criterion.

The match criterion is not configured by default.

This command is one of the if-match clauses of routing policy, used for matching routes with the specified route cost.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit routing information with a cost of 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match cost 8
```

if-match extcommunity

Syntax **if-match extcommunity** *ext-comm-list-number*&<1-16>

undo if-match extcommunity [*ext-comm-list-number*&<1-16>]

View Routing policy view

Parameters *ext-comm-list-number*: Extended community list number, in the range of 1 to 199.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match extcommunity** command to specify extended community list(s) for matching against the extended community attribute of routing information.

Use the **undo if-match extcommunity** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Match the extended community attribute of routes against extended community lists 100 and 150.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match extcommunity 100 150
```

if-match interface

Syntax **if-match interface** { *interface-type interface-number* }&<1-16>

undo if-match interface [*interface-type interface-number*]&<1-16>

View Routing policy view

Parameters *interface-type*: Interface type

interface-number: Interface number

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **if-match interface** command to specify interface(s) for matching against the outbound interfaces of routing information.

Use the **undo if-match interface** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit the routing information with the outbound interface as Ethernet1/0.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match interface ethernet 1/0
```

if-match mpls-label

Syntax **if-match mpls-label**

undo if-match mpls-label

View Routing policy view

Parameters None

Description Use the **if-match mpls-label** command to specify the MPLS label match criterion.

Use the **undo if-match mpls-label** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Match MPLS label of routing updates.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match mpls-label
```

if-match route-type

Syntax **if-match route-type** { **internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2** } *

undo if-match route-type [**internal** | **external-type1** | **external-type2** | **external-type1or2** | **is-is-level-1** | **is-is-level-2** | **nssa-external-type1** | **nssa-external-type2** | **nssa-external-type1or2**] *

View Routing policy view

Parameters **internal**: Internal routes (OSPF intra-area and inter-area routes).

external-type1: OSPF Type 1 external routes.

external-type2: OSPF Type 2 external routes.

external-type1or2: OSPF Type 1 or 2 external routes.

is-is-level-1: IS-IS Level-1 routes.

is-is-level-2: IS-IS Level-2 routes.

nssa-external-type1: OSPF NSSA Type 1 external routes.

nssa-external-type2: OSPF NSSA Type 2 external routes.

nssa-external-type1or2: OSPF NSSA Type 1 or 2 external routes.

Description Use the **if-match route-type** command to configure a route type match criterion.

Use the **undo if-match route-type** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to match internal routes.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match route-type internal
```

if-match tag

Syntax **if-match tag** *value*

undo if-match tag

View Routing policy view

Parameters *value*: Specifies a tag value, ranging from 0 to 4294967295.

Description Use the **if-match tag** command to specify a tag for matching against the tag field of the routes.

Use the **undo if-match tag** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin** and **apply tag**.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit RIP, OSPF and IS-IS routing information with the tag as 8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match tag 8
```

ip as-path

Syntax **ip as-path** *as-path-number* { **deny** | **permit** } *regular-expression*

undo ip as-path *as-path-number*

View System view

Parameters *as-path-number*: AS path ACL number, in the range of 1 to 256.

deny: Specifies the matching mode for the AS path ACL as deny.

permit: Specifies the matching mode for the AS path ACL as permit.

regular-expression: Regular expression of AS path, a string of 1 to 50 characters.

BGP routing information contains the AS path attribute field that identifies the autonomous systems through which routing information has passed. Used to compare with the AS path attribute, a regular expression is a formula comprised of characters, for example, ^200. *100$, which matches AS path attribute fields that start with AS200 and end with AS100.

The meanings of special characters used in regular expressions are shown below:

Character	Meaning
.	Matches any single character, including blank space.
*	Matches 0 or more patterns.
+	Matches 1 or more patterns.
^	Matches the beginning of an input string.
$	Matches the end of an input string.
_	Matches a comma, left brace, right brace, left parenthesis, right parenthesis, the beginning of an input string, the end of an input string, or a space.
[range]	Means the range of single-character patterns.
-	Separates the ending points of a range.

Description Use the **ip as-path** command to create an AS path ACL.

Use the **undo ip as-path** command to remove an AS path ACL.

No AS path ACL is created by default.

Examples # Create an AS path ACL numbered 1, permitting routing information whose AS_PATH starts with 10.

```
<Sysname> system-view
[Sysname] ip as-path 1 permit ^10
```

ip community-list

Syntax **ip community-list** *basic-comm-list-num* { **deny** | **permit** } [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

undo ip community-list *basic-comm-list-num* [*community-number-list*] [**internet** | **no-advertise** | **no-export** | **no-export-subconfed**] *

ip community-list *adv-comm-list-num* { **deny** | **permit** } *regular-expression*

undo ip community-list *adv-comm-list-num* [*regular-expression*]

View System view

Parameters *basic-comm-list-num*: Basic community list number, in the range 1 to 99.

adv-comm-list-num: Advanced community list number, in the range 100 to 199.

regular-expression: Regular expression of advanced community attribute, a string of 1 to 50 characters.

deny: Specifies the matching mode of the community list as deny.

permit: Specifies the matching mode of the community list as permit.

community-number-list: Community number list, in the *community number* or *aa:nn* format, with *community number* in the range 1 to 4294967295 and *aa* and *nn* in the range 0 to 65535. Each format can be entered up to 16 times.

internet: Routes with this attribute can be advertised to all the BGP peers. By default, all routes have this attribute.

no-advertise: Routes with this attribute will not be advertised to other BGP peers.

no-export: Routes with this attribute will not be advertised out the local AS, or the confederation but can be advertised to other ASs in the confederation.

no-export-subconfed: Routes with this attribute cannot be advertised out the local AS, or to other sub ASs in the confederation.

Description Use the **ip community-list** to define a community list entry.

Use the **undo ip community-list** command to remove a community list or entry.

No community list is defined by default.

Examples # Define basic community list 1 to permit routing information with the **internet** community attribute.

```
<Sysname> system-view
[Sysname] ip community-list 1 permit internet
```

Define advanced community list 100 to permit routing information with the community attribute starting with 10.

```
<Sysname> system-view
[Sysname] ip community-list 100 permit ^10
```

ip extcommunity-list

Syntax **ip extcommunity-list** *ext-comm-list-number* { **deny** | **permit** } { **rt** *route-target* }&<1-16>

undo ip extcommunity-list *ext-comm-list-number*

View System view

Parameters *ext-comm-list-number*: Extended community list number, in the range 1 to 199.

permit: Specifies the matching mode for the extended community list as permit.

deny: Specifies the matching mode for the extended community list as deny.

rt *route-target*: Specifies route target extended community attribute, which is a string of 3 to 21 characters. *route-target* has two forms:

A 16-bit AS number: a 32-bit self-defined number, for example, 101:3;

A 32-bit IP address: a 16-bit self-defined number, for example, 192.168.122.15:1.

&<1-16>: Indicates the argument before it can be entered up to 16 times.

Description Use the **ip extcommunity-list** to define an extended community list entry.

Use the **undo ip extcommunity-list** command to remove an extended community list.

No extended community list is defined by default.

Examples # Define extended community list 1 to permit routing information with RT 200:200.

```
<Sysname> system-view
[Sysname] ip extcommunity-list 1 permit rt 200:200
```

route-policy

Syntax **route-policy** *route-policy-name* { **permit** | **deny** } **node** *node-number*

undo route-policy *route-policy-name* [**node** *node-number*]

View System view

Parameters *route-policy-name*: Routing policy name, a string of 1 to 19 characters.

permit: Specifies the matching mode of the routing policy node as permit. If a route satisfies all the if-match clauses of the node, it passes through the filtering of the node and then is executed with the apply clauses of the node. If not, it goes to the next node of the routing policy.

deny: Specifies the matching mode of the routing policy node as deny. If a route satisfies all the if-match clauses of the node, it does not pass the filtering of the node and will not go to the next node.

node *node-number*: Node number, in the range 0 to 65535. The node with a smaller *node-number* will be tested first when the routing policy is used for filtering routing information.

Description Use the **route-policy** command to create a routing policy and enter its view.

Use the **undo route-policy** command to remove a routing policy.

No routing policy is created by default.

A routing policy is used for routing information filtering or policy routing. It contains several nodes and each node comprises some if-match and apply clauses. The if-match clauses define the matching criteria of the node and the apply clauses define the actions performed after a packet passes the filtering of the node. The relation among the if-match clauses of a node is logic AND, namely all the if-match clauses must be satisfied. The filter relation among different route-policy nodes is logic OR, namely a packet passing a one node passes the routing policy.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **apply ip-address next-hop**, **apply local-preference**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy 1 with node 10 and matching mode as permit, and then enter routing policy view.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy]
```

79 IPv4 Routing Policy Configuration Commands

apply ip-address next-hop

Syntax **apply ip-address next-hop** *ip-address*

undo apply ip-address next-hop

View Routing policy view

Parameters *ip-address*: IP address of the next hop.

Description Use the **apply ip-address next-hop** command to set a next hop for IPv4 routing information.

Use the **undo apply ip-address next-hop** command to remove the clause configuration.

No next hop address is set for IPv4 routing information by default.

It is invalid to use the **apply ip-address next-hop** command to set a next hop when redistributing routes.

Related commands: **if-match interface**, **if-match acl**, **if-match ip-prefix**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply local-preference**, **apply cost**, **apply origin** and **apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode **permit**. If passing AS path ACL 1, a route's next hop is set to 193.1.1.8.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ip-address next-hop 193.1.1.8
```

display ip ip-prefix

Syntax **display ip ip-prefix** [*ip-prefix-name*]

View Any view

Parameters *ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

Description Use the **display ip ip-prefix** command to display the statistics of an IPv4 address prefix list. If no ip-prefix-name is specified, statistics for all IPv4 address prefix lists will be displayed.

Related commands: **ip ip-prefix**.

Examples # Display the statistics of IPv4 prefix list **abc**.

```
<Sysname> display ip ip-prefix abc
Prefix-list abc
Permitted 0
Denied 0
        index: 10               permit  1.0.0.0/11              ge  22  le  32
```

Table 285 Description on the fields of the display ip ip-prefix command.

Field	Description
Prefix-list	Name of the IPv4 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
index	Internal serial number of the IPv4 prefix list
permit	Matching mode: permit or deny
1.0.0.0/11	Match IP address and mask
ge	greater-equal, the lower limit mask
le	less-equal, the upper limit mask

if-match acl

Syntax **if-match acl** *acl-number*

undo if-match acl

View Routing policy view

Parameters *acl-number*: ACL number from 2000 to 3999.

Description Use the **if-match acl** command to configure an ACL match criterion.

Use the **undo if-match** command to remove the match criterion.

No ACL match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**,**apply tag**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit routes matching ACL 2000.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match acl 2000
```

if-match ip

Syntax **if-match ip** { **next-hop** | **route-source** } { **acl** *acl-number* | **ip-prefix** *ip-prefix-name* }

undo if-match ip { **next-hop** | **route-source** } [**acl** | **ip-prefix**]

View Routing policy view

Parameters **next-hop**: Matches next hop.

route-source: Matches source address.

acl *acl-number*: Matches an ACL with a number from 2000 to 2999.

ip-prefix *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description Use the **if-match ip** command to configure a next hop or source address match criterion for IPv4 routes.

Use the **undo if-match ip** command to remove the match criterion.

The match criterion is not configured by default.

Related commands: **route-policy**.

Examples # Create routing policy **policy1** with node 10, matching mode as permit. Define an if-match clause to permit routing information whose next hop address matches IP prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ip next-hop ip-prefix p1
```

if-match ip-prefix

Syntax **if-match ip-prefix** *ip-prefix-name*

undo if-match ip-prefix

View Routing policy view

Parameters *ip-prefix-name*: Matches an IP prefix list with a name being a string of 1 to 19 characters.

Description Use the **if-match ip-prefix** command to configure an IP prefix list based match criterion.

Use the **undo if-match ip-prefix** command to remove the match criterion.

No IP prefix list based match criterion is configured by default.

Related commands: **if-match interface**, **if-match ip next-hop**, **if-match cost**, **if-match tag**, **route-policy**, **apply ip-address next-hop**, **apply cost**, **apply local-preference**, **apply origin**, **apply tag**.

Examples # Create routing policy **policy2** with node 10, matching mode as **permit**. Define an if-match clause to permit routes whose destination addresses match IP prefix list **p1**.

```
<Sysname> system-view
[Sysname] route-policy policy2 permit node 10
[Sysname-route-policy] if-match ip-prefix p1
```

ip ip-prefix

Syntax **ip ip-prefix** *ip-prefix-name* [**index** *index-number*] { **permit** | **deny** } *ip-address mask-length* [**greater-equal** *min-mask-length*] [**less-equal** *max-mask-length*]

undo ip ip-prefix *ip-prefix-name* [**index** *index-number*]

View System view

Parameters *ip-prefix-name*: IPv4 prefix list name, a string of 1 to 19 characters.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an item of the IPv4 prefix list. The index with a smaller number is tested first.

permit: Specifies the matching mode for the IPv4 prefix list as permit, that is, when a route to be filtered is in the range of the IPv4 prefix list, the route passes the IPv4 prefix list without needing to enter the next item for testing. If the route to be filtered is not in the prefix range, it will enter the next item test.

deny: Specifies the matching mode for the IPv4 prefix list as deny, that is, when a route to be filtered is in the IPv4 prefix list range, the route neither passes the filter nor enters the next node for testing. If not in the range, the route will enter the next item test.

ip-address mask-length: Specifies an IPv4 address prefix and mask length. The *mask-length* is in the range 0 to 32.

min-mask-length, *max-mask-length*: Specifies the range for prefix if the IPv4 address and prefix length are matched. **greater-equal** means "greater than or equal to" and **less-equal** means "less than or equal to". The range relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32. If only *min-mask-length* is specified, the prefix length range is [min-mask-length, 32]. If only *max-mask-length* is specified, the prefix length range is [mask-length, max-mask-length]. If both min-mask-length and max-mask-length are specified, the prefix length range is [min-mask-length, max-mask-length].

Description Use the **ip ip-prefix** command to configure an IPv4 prefix list item.

Use the **undo ip ip-prefix** command to remove an IPv4 prefix list or an item.

No IPv4 prefix list is configured by default.

An IPv4 prefix list is used to filter IPv4 addresses. It may have multiple items, each of which specifies a range of IPv4 prefix. The filtering relation among items is logic OR, namely, passing any item means the IPv4 prefix list is passed. If no item is passed, the IP prefix list cannot be passed.

The IP prefix range is determined by *mask-length* and [*min-mask-length, max-mask-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, then the IP address to be filtered must satisfy both of them.

If *ip-address mask-length* is specified as 0.0.0.0 0, then only the default routes will be matched.

To match all the routes, use 0.0.0.0 0 **less-equal** 32.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an IP prefix list named p1 to permit only the routes in the network segment 10.0.192.0/8 and with mask length 17 or 18.

```
<Sysname> system-view
[Sysname] ip ip-prefix p1 permit 10.0.192.0 8 greater-equal 17 less-equal 18
```

reset ip ip-prefix

Syntax **reset ip ip-prefix** [*ip-prefix-name*]

View User view

Parameters *ip-prefix-name*: IP prefix list name, a string of 1 to 19 characters.

Description Use the **reset ip ip-prefix** command to clear the statistics of a specified IPv4 prefix list. If no *ip-prefix-name* is specified, the statistics of all the IPv4 prefix lists will be cleared.

Examples # Clear the statistics of IPv4 prefix list **abc**.

```
<Sysname> reset ip ip-prefix abc
```

80 IPv6 Routing Policy Configuration Commands

apply ipv6 next-hop

Syntax **apply ipv6 next-hop** *ipv6-address*

undo apply ipv6 next-hop

View Routing policy view

Parameters *ipv6-address*: Next hop IPv6 address.

Description Use the **apply ipv6 next-hop** command to apply a next hop to IPv6 routes.

Use the **undo apply ipv6 next-hop** command to remove the clause configuration.

No next hop address is set for IPv6 routing information by default.

Using the **apply ipv6 next-hop** command to set a next hop when redistributing routes does not take effect.

Examples # Create routing policy **policy1** with node 10, matching mode **permit**. If a route matches AS path ACL 1, set next hop 3ff3:506::1 for it.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match as-path 1
[Sysname-route-policy] apply ipv6 next-hop 3ffe:506::1
```

display ip ipv6-prefix

Syntax **display ip ipv6-prefix** [*ipv6-prefix-name*]

View Any view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **display ip ipv6-prefix** command to display the statistics of the specified IPv6 prefix list. If no IPv6 prefix list is specified, the statistics of all the IPv6 prefix lists will be displayed.

Examples # Display the statistics of all the IPv6 prefix lists.

```
<Sysname> display ip ipv6-prefix
Prefix-list6 abc
Permitted 0
Denied 0
         index:   10            permit  ::/0
         index:   20             permit  ::/1                ge  1   le  128
```

Table 286 Description on the fields of the display ip ipv6-prefix command

Field	Description
Prefix-list6	Name of the IPv6 prefix list
Permitted	Number of routes satisfying the match criterion
Denied	Number of routes not satisfying the match criterion
Index	Internal serial number of address prefix list
Permit	Matching mode: permit, deny
::/1	IPv6 address and its prefix length for matching
ge	greater-equal, the lower limit prefix length
Le	less-equal, the upper limit prefix length

if-match ipv6

Syntax **if-match ipv6** { **address** | **next-hop** | **route-source** } { **acl** *acl6-number* | **prefix-list** *ipv6-prefix-name* }

undo if-match ipv6 { **address** | **next-hop** | **route-source** } [**acl** | **prefix-list**]

View Routing policy view

Parameters **address**: Matches the destination address of IPv6 routing information.

next-hop: Matches the next hop of IPv6 routing information.

route-source: Matches the source address of IPv6 routing information.

acl *acl6-number*: Specifies the number of an IPv6 ACL for filtering, in the range 2000 to 3999 for **address**, and 2000 to 2999 for **next-hop** and **route-source**.

prefix-list *ipv6-prefix-name*: Specifies the name of a IPv6 prefix list for filtering, a string of 1 to 19 characters.

Description Use the **if-match ipv6** command to configure a destination, next hop or source address based match criterion for IPv6 routes.

Use the **undo if-match ipv6** command to remove the match criterion.

The match criterion is not configured by default.

Examples # Create a routing policy named policy1 with node 10, matching mode as permit. Define an if-match clause to permit the routing information whose next hop address matches IPv6 prefix list p1.

```
<Sysname> system-view
[Sysname] route-policy policy1 permit node 10
[Sysname-route-policy] if-match ipv6 next-hop prefix-list p1
```

ip ipv6-prefix

Syntax

ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*] { **deny** | **permit** } *ipv6-address prefix-length* [**greater-equal** *min-prefix-length*] [**less-equal** *max-prefix-length*]

undo ip ipv6-prefix *ipv6-prefix-name* [**index** *index-number*]

View System view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters, for uniquely specifying an IPv6 prefix list.

index-number: Index number, in the range 1 to 65535, for uniquely specifying an IPv6 prefix list item. The item with a smaller *index-number* will be tested first.

permit: Specifies the matching mode for the IPv6 prefix list as permit, that is, if a route matches the IPv6 prefix list, it passes the IPv6 prefix list without needing to enter the next item for test. If not, it will enter the next item test.

deny: Specifies the matching mode for the IPv6 prefix list as deny, that is, if a route matches the IPv6 prefix list, the route neither passes the filter nor enters the next node for test. If not, the route will enter the next item test.

ipv6-address prefix-length: Specifies an IPv6 prefix and prefix length, with *prefix-length* being in the range 0 to 128. When specified as :: 0, it matches the default route.

greater-equal *min-prefix-length:* Greater than or equal to the minimum prefix length.

less-equal *max-prefix-length*: Less than or equal to the maximum prefix length.

The length relation is *mask-length* <= *min-mask-length* <= *max-mask-length* <= 32. If only min-prefix-length is specified, the prefix length range is [min-prefix-length, 128]. If only max-prefix-length is specified, the prefix length range is [prefix-length, max-prefix-length]. If both min-prefix-length and max-prefix-length are specified, the prefix length range is [min-prefix-length, max-prefix-length].

Description Use the **ip ipv6-prefix** command to configure an IPv6 prefix list item.

Use the **undo ip ipv6-prefix** command to remove an IPv6 prefix list or an item.

No IPv6 prefix list is configured by default.

The IPv6 address prefix list is used to filter IPv6 addresses. It may have multiple items, and each of them specifies a range of IPv6 prefix. The filtering relation among items is logic OR, namely, a route passing an item will pass the prefix list.

The IPv6 prefix range is determined by *prefix-length* and [*min-prefix-length, max-prefix-length*]. If both *mask-length* and [*min-mask-length, max-mask-length*] are specified, then the IPv6 addresses must satisfy both of them.

If *ipv6-address prefix-length* is specified as :: 0, then only the default route matches.

If you want to it match all the routes, configure it as :: 0 **less-equal** 128.

Examples # Permit the IPv6 addresses with mask length between 32 bits and 64 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit :: 0 greater-equal 32 less-equal 64
```

Deny the IPv6 addresses with prefix as 3FFE:D00::/32, prefix length greater than or equal to 32 bits.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc deny 3FEE:D00:: 32 less-equal 128
```

reset ip ipv6-prefix

Syntax **reset ip ipv6-prefix** [*ipv6-prefix-name*]

View User view

Parameters *ipv6-prefix-name*: IPv6 prefix list name, a string of 1 to 19 characters.

Description Use the **reset ip ipv6-prefix** command to clear the statistics of the specified IPv6 prefix list. If no name is specified, the statistics of all IPv6 prefix lists will be cleared.

Examples # Clear the statistics of IPv6 prefix list **abc**.

```
<Sysname> reset ip ipv6-prefix abc
```

81 STATIC ROUTING CONFIGURATION COMMANDS

delete static-routes all

Syntax **delete** [**vpn-instance** *vpn-instance-name*] **static-routes all**

View System view

Parameters *vpn-instance-name*: Name of a VPN instance, a string of 1 to 31 case-sensitive characters.

Description Use the **delete static-routes all** command to delete all static routes.

When you use this command to delete static routes, the system will prompt you to confirm the operation before deleting all the static routes.

Related commands: **display ip routing-table** on page 929 and **ip route-static**.

Examples # Delete all static routes on the router.

```
<Sysname> system-view
[Sysname] delete static-routes all
This will erase all ipv4 static routes and their configurations, you must reconf
igure all static routes
Are you sure?[Y/N]:Y
```

ip route-static

Syntax **ip route-static** *dest-address* { *mask* | *mask-length* } { *gateway-address* [**track** *track-entry-number*] | *interface-type interface-number* | **vpn-instance** *d-vpn-instance-name gateway-address* [**track** *track-entry-number*] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static *dest-address* { *mask* | *mask-length* } [*gateway-address* | *interface-type interface-number* [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address*] [**preference** *preference-value*]

ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } { *gateway-address* [**track** *track-entry-number*] [**public**] | *interface-type interface-number* | **vpn-instance** *d-vpn-instance-name gateway-address* [**track** *track-entry-number*] } [**preference** *preference-value*] [**tag** *tag-value*] [**description** *description-text*]

undo ip route-static vpn-instance *s-vpn-instance-name*&<1-6> *dest-address* { *mask* | *mask-length* } [*gateway-address* [**public**] | *interface-type interface-number* [*gateway-address*] | **vpn-instance** *d-vpn-instance-name gateway-address*] [**preference** *preference-value*]

View System view

Parameters **vpn-instance** *s-vpn-instance-name*&<1-6>: Specifies the VPN instance name, which is a string of 1 to 31 case-sensitive characters. &<1-6> indicates the argument before it can be entered up to 6 times. Each VPN instance has its own routing table, and the configured static route is installed in the routing tables of the specified VPN instances.

dest-address: Destination IP address of the static route, in dotted decimal notation.

mask: Mast of the IP address, in dotted decimal notation.

mask-length: Mask length, in the range 0 to 32.

gateway-address: IP address of the next hop, in dotted decimal notation.

interface-type interface-number: Specifies the output interface by its type and number. If the output interface is a broadcast interface, such as an Ethernet interface, a virtual template or a VLAN interface, the next hop address must be specified.

vpn-instance *d-vpn-instance-name*: Name of the destination VPN instance, case-sensitive. If a destination VPN instance name is specified, the router will search the output interface in the destination VPN instance based on the configured *gateway-address*.

gateway-address **public**: Indicates that the specified *gateway-address* is a public network address, rather than a VPN instance address.

preference *preference-value* : Specifies the preference of the static route, which is in the range of 1 to 255 and defaults to 60.

tag *tag-value*: Sets a tag value for the static route. Tags of routes are used in routing policies to control routing. For information about routing policy, refer to "Routing Policy Common Configuration Commands" on page 1187.

description *description-text*: Configures a description for the static route, which consists of 1 to 60 characters, including special characters like space, but excluding "?".

track *track-entry-number*: Associates the static route with a track entry. Use the *track-entry-number* argument to specify a track entry number, in the range 1 to 1024. Support for this argument varies with devices.

Description Use the **ip route-static** command to configure a unicast static route.

Use the **undo ip route-static** command to delete a unicast static route.

When configuring a unicast static route, note that:

1. If the destination IP address and the mask are both 0.0.0.0, the configured route is a default route. If routing table searching fails, the router will use the default route for packet forwarding.
2. Different route management policies can be implemented for different route preference configurations. For example, specifying the same preference for different routes to the same destination address enables load sharing, while specifying different preferences for these routes enables route backup.
3. When configuring a static route, you can specify the output interface or the next hop address based on the actual requirement. Note that the next hop address must not be the IP address of the local interface; otherwise, the route configuration will not take effect. For interfaces that support network address to link layer address resolution or point-to-point interfaces, you can specify the output interface or next hop address. When specifying the output interface, note that:
   - For a NULL0 or loopback interface, if the output interface has already been configured, there is no need to configure the next hop address.
   - For point-to-point interfaces, you can specify the output interface if you do not know the peer address. Thus, there is no need to change the router's configuration even if the peer address is changed. A PPP interface obtains the peer's IP address through PPP negotiation. In this case, you need only specify the output interface.
   - For NBMA and P2MP interfaces, which support point-to-multipoint networks, the IP address to link layer address mapping must be established in addition to IP route configuration. In general, it is recommended to configure the next hop IP address when you configure the output interface.
   - It is not recommended to specify a broadcast interface (such as an Ethernet interface, virtual template, or VLAN interface) as the output interface for a static route, because a broadcast interface may have multiple next hops. If you have to do so, you must specify the corresponding next hop of the interface at the same time.

Related commands: **display ip routing-table** on page 929 and **ip route-static default-preference**.

- *The static route does not take effect if you specify its next hop address first and then configure the address as the IP address of a local interface, such as Ethernet interface and VLAN interface.*
- *To configure track monitoring for an existing static route, simply associate the static route with a track entry. For a non-existent static route, configure it and associate it with a Track entry.*
- *If the track module uses NQA to detect the reachability of the private network static route's nexthop, the VPN instance number of the static route's nexthop must be identical to that configured in the NQA test group.*
- *If a static route needs route recursion, the associated track entry must monitor the nexthop of the recursive route instead of that of the static route; otherwise, a valid route may be mistakenly considered invalid.*

Examples # Configure a static route, whose destination address is 1.1.1.1/24, next hop address is 2.2.2.2, tag value is 45, and description information is "**for internet & intranet**".

```
<Sysname> system-view
[Sysname] ip route-static 1.1.1.1 24 2.2.2.2 tag 45 description for
internet & intranet
```

Configure a static route for a VPN instance named **vpn1**: the destination address is 1.1.1.1/16 and the next hop address is 1.1.1.2, which is the address of this VPN instance.

```
<Sysname> system-view
[Sysname] ip route-static vpn-instance vpn1 1.1.1.1 16 vpn-instance
vpn1 1.1.1.2
```

ip route-static default-preference

Syntax **ip route-static default-preference** *default-preference-value*

undo ip route-static default-preference

View System view

Parameters *default-preference-value*: Default preference for static routes, which is in the range of 1 to 255.

Description Use the **ip route-static default-preference** command to configure the default preference for static routes.

Use the **undo ip route-static default-preference** command to restore the default.

By default, the default preference of static routes is 60.

Note that:

- If no preference is specified when configuring a static route, the default preference is used.
- When the default preference is re-configured, it applies to newly added static routes only.

Related commands: **display ip routing-table** on page 929 and **ip route-static**.

Examples # Set the default preference of static routes to 120.

```
<Sysname> system-view
[Sysname] ip route-static default-preference 120
```

82 IPv6 BGP CONFIGURATION COMMANDS

balance (IPv6 address family view)

Syntax **balance** *number*

undo balance

View IPv6 address family view

Parameters *number*: Number of BGP routes participating in load balancing, in the range 1 to 8. When it is set to 1, no load balancing is available.

Description Use the **balance** command to configure the number of routes participating in IPv6 BGP load balancing.

Use the **undo balance** command to restore the default.

The feature is not available by default.

Unlike IGP, BGP has no explicit metric for making load balancing decision. Instead, it implements load balancing by defining its routing rule.

Related commands: **display ipv6 routing-table** on page 942.

Examples # Set the number of routes participating in IPv6 BGP load balancing to 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] balance 2
```

bestroute as-path-neglect (IPv6 address family view)

Syntax **bestroute as-path-neglect**

undo bestroute as-path-neglect

View IPv6 address family view

Parameters None

Description Use the **bestroute as-path-neglect** command to configure the IPv6 BGP router to not evaluate the AS_PATH during best route selection.

Use the **undo bestroute as-path-neglect** command to configure the IPv6 BGP router to use the AS_PATH during best route selection.

By default, the router takes AS_PATH as a factor when selecting the best route.

Examples # Ignore AS_PATH in route selection.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute as-path-neglect
```

bestroute compare-med (IPv6 address family view)

Syntax **bestroute compare-med**

undo bestroute compare-med

View IPv6 address family view

Parameters None

Description Use the **bestroute compare-med** command to enable the comparison of the MED for paths from each AS.

Use the **undo bestroute compare-med** command to disable this comparison.

This comparison is not enabled by default.

Examples # Compare the MED for paths from an AS for selecting the best route.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute compare-med
```

bestroute med-confederation (IPv6 address family view)

Syntax **bestroute med-confederation**

undo bestroute med-confederation

View IPv6 address family view

Parameters None

Description Use the **bestroute med-confederation** command to enable the comparison of the MED for paths from confederation peers for best route selection.

Use the **undo bestroute med-confederation** command to disable the comparison.

By default, this comparison is not enabled.

With this feature enabled, the system can only compare the MED for paths from peers within the confederation. Paths from external ASs are advertised throughout the confederation without MED comparison.

Examples # Compare the MED for paths from peers within the confederation.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] bestroute med-confederation
```

compare-different-as-med (IPv6 address family view)

Syntax **compare-different-as-med**

undo compare-different-as-med

View IPv6 address family view

Parameters None

Description Use the **compare-different-as-med** command to enable the comparison of the MED for paths from peers in different ASs.

Use the **undo compare-different-as-med** command to disable the comparison.

The comparison is disabled by default.

If there are several paths available for one destination, the path with the smallest MED value is selected.

Do not use this command unless associated ASs adopt the same IGP protocol and routing selection method.

Examples # Enable to compare the MED for paths from peers in different ASs.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] compare-different-as-med
```

dampening (IPv6 address family view)

Syntax **dampening** [*half-life-reachable half-life-unreachable reuse suppress ceiling* | **route-policy** *route-policy-name*] *

undo dampening

View IPv6 address family view

Parameters *half-life-reachable*: Specifies the half-life for active routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

half-life-unreachable: Specifies the half-life for active routes, in the range 1 to 45 minutes. By default, the value is 15 minutes.

reuse: Specifies the reuse threshold value for suppressed routes, in the range 1 to 20000. Penalty value of a suppressed route decreasing under the value is reused. By default, its value is 750.

suppress: Specifies a suppression threshold from 1 to 20000, which should be bigger than the *reuse* value. Routes with a penalty value bigger than the threshold are suppressed. By default, it is 2000.

ceiling: Specifies a ceiling penalty value from 1001 to 20000. The value must be bigger than the *suppress* value. By default, the value is 16000.

route-policy-name: Routing policy name, a string of 1 to 19 characters.

half-life-reachable, half-life-unreachable, reuse, suppress and *ceiling* are mutually dependent. Once any one is configured, all the others should also be specified accordingly.

Description Use the **dampening** command to enable IPv6 BGP route dampening or/and configure dampening parameters.

Use the **undo dampening** command to disable route dampening.

By default, no route dampening is configured.

Related commands: **reset bgp ipv6 dampening**, **reset bgp ipv6 flap-info**, **display bgp ipv6 routing-table dampened**, **display bgp ipv6 routing-table dampening parameter** and **display bgp ipv6 routing-table flap-info**.

Examples # Enable IPv6 BGP route dampening and configure route dampening parameters.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] dampening 10 10 1000 2000 3000
```

default local-preference(IPv6 address family view)

Syntax **default local-preference** *value*

undo default local-preference

View IPv6 address family view

Parameters *value*: Default local preference, in the range 0 to 4294967295. The larger the value is, the higher the preference is.

Description Use the **default local-preference** command to configure the default local preference.

Use the **undo default local-preference** command to restore the default value.

By default, the default local preference is 100.

Use this command to affect IPv6 BGP route selection.

Examples # Two devices A and B in the same AS are connected to another AS. Change the local preference of B from default value 100 to 180, making the route passing B preferred.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default local-preference 180
```

default med (IPv6 address family view)

Syntax **default med** *med-value*

undo default med

View IPv6 address family view

Parameters *med-value*: MED value, in the range 0 to 4294967295.

Description Use the **default med** command to specify the default MED value.

Use the **undo default med** command to restore the default.

By default, the default *med-value* is 0.

The multi-exit discriminator (MED) is an external metric of a route. Different from local preference, MED is exchanged between ASs and will stay in the AS once it enters the AS. The route with a lower MED is preferred. When a router running BGP obtains several routes with the identical destination and different next-hops from various external peers, it will select the best route depending on the MED

value. In the case that all other conditions are the same, the system first selects the route with the smaller MED value as the best route for the autonomous system.

Examples # Devices A and B belong to AS100 and device C belongs to AS200. C is the peer of A and B. Configure the MED of A as 25 to make C select the path from B.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default med 25
```

default-route imported (IPv6 address family view)

Syntax **default-route imported**

undo default-route imported

View IPv6 address family view

Parameters None

Description Use the **default-route imported** command to enable the redistribution of default route into the IPv6 BGP routing table.

Use the **undo default-route imported** command to disable the redistribution.

By default, the redistribution is not enabled.

Examples # Enable the redistribution of default route from OSPFv3 into IPv6 BGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] default-route imported
[Sysname-bgp-af-ipv6] import-route ospfv3 1
```

display bgp ipv6 group

Syntax **display bgp ipv6 group** [*ipv6-group-name*]

View Any view

Parameters *ipv6-group-name*: Peer group name, a string of 1 to 47 characters.

Description Use the **display bgp ipv6 group** command to display IPv6 peer group information.

If no *ipv6-group-name* is specified, information about all peer groups is displayed.

Examples # Display the information of the IPv6 peer group **aaa**.

```
<Sysname> display bgp ipv6 group aaa

 BGP peer-group is aaa
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 4294967295
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 0
 No routing policy is configured
  Members:
  Peer        V    AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State

  20:20::20:1  4   200       170       141      0        2 02:13:35 Established
```

Table 287 Description on the fields of the display bgp ipv6 group command

Field	Description
BGP peer-group	Name of the peer group
remote AS	AS number of the peer group
Type	Type of the peer group
Maximum allowed prefix number	Maximum allowed prefix number
Threshold	Threshold value
hold timer value	Holdtime
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum interval between advertisements
Peer Preferred Value	Preferred value of the routes from the peer
No routing policy is configured	No routing policy is configured for the peer
Members	Group members
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	State machine of peer

display bgp ipv6 network

Syntax **display bgp ipv6 network**

View Any view

Parameters None

Description Use the **display bgp ipv6 network** command to display IPv6 routes advertised with the **network** command.

Examples # Display IPv6 routes advertised with the **network** command.

```
<Sysname> display bgp ipv6 network
  BGP Local Router ID is 1.1.1.2.
  Local AS Number is 200.
  Network          Mask            Route-policy        Short-cut

  2002::           64
  2001::           64                                  Short-cut
```

Table 288 Description on the fields of the display bgp ipv6 network command

Field	Description
BGP Local Router ID	BGP Local Router ID
Local AS Number	Local AS Number
Network	Network address
Prefix	Prefix length
Route-policy	Routing policy
Short-cut	Shortcut route

display bgp ipv6 paths

Syntax **display bgp ipv6 paths** [*as-regular-expression*]

View Any view

Parameters *as-regular-expression*: AS path regular expression.

Description Use the **display bgp ipv6 paths** command to display IPv6 BGP path information.

If no parameter is specified, all path information will be displayed.

Examples # Display IPv6 BGP path information.

```
<Sysname> display bgp ipv6 paths

    Address        Hash     Refcount  MED          Path/Origin
    0x5917098      1        1          0             i
    0x59171D0      9        2          0             100i
```

Table 289 Description on the fields of the display bgp ipv6 paths command

Field	Description
Address	Route destination address in local database, in dotted hexadecimal notation
Hash	Hash index
Refcount	Count of routes that used the path
MED	MED of the path

Table 289 Description on the fields of the display bgp ipv6 paths command

Field	Description	
Path	AS_PATH attribute of the path, recording the ASs it has passed, for avoiding routing loops	
Origin	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates the route is interior to the AS. Summary routes and routes defined using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 peer

Syntax **display bgp ipv6 peer** [*group-name* **log-info** | *ipv4-address* **verbose** | *ipv6-address* { **log-info** | **verbose** }]

View Any view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

Ipv4-address: IPv4 address of a peer.

ipv6-address: Specifies the IPv6 address of a peer to be displayed.

log-info: Displays log information of the specified peer.

verbose: Displays the detailed information of the peer.

Description Use the **display bgp ipv6 peer** command to display peer/peer group information.

If no parameter specified, information about all peers and peer groups is displayed.

Examples # Display all IPv6 peer information.

```
<Sysname> display bgp ipv6 peer

 BGP Local router ID : 20.0.0.1
 local AS number : 100
Total number of peers : 1                 Peers in established state : 1

Peer      V    AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down    State

20::21    4   200  17       19       0          3  00:09:59   Established
```

Table 290 Description on the fields of the display bgp ipv6 peer command

Field	Description
Peer	IPv6 address of the peer
V	Peer BGP version
AS	AS number
MsgRcvd	Messages received
MsgSent	Messages sent
OutQ	Messages to be sent
PrefRcv	Number of prefixes received
Up/Down	The lasting time of a session/the lasting time of present state (when no session is established)
State	Peer state

display bgp ipv6 routing-table

Syntax **display bgp ipv6 routing-table** [*ipv6-address prefix-length*]

View Any view

Parameters *ipv6-address*: Destination IPv6 address.

prefix-length: Prefix length of the IPv6 address, in the range 0 to 128.

Description Use the **display bgp ipv6 routing-table** command to display IPv6 BGP routing table information.

Examples # Display the IPv6 BGP routing table.

```
<Sysname> display bgp ipv6 routing-table

 Total Number of Routes: 2

 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i

 *>  Network : 40:40::                                  PrefixLen : 64
     NextHop : 40:40::40:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Table 291 Description on the fields of the display bgp ipv6 routing-table command

Field	Description
Local router ID	Local router ID

Table 291 Description on the fields of the display bgp ipv6 routing-table command

Field	Description	
Status codes	Status codes: * - valid > - best d - damped h - history i - internal (IGP) s - summary suppressed (suppressed) S - Stale	
Origin	i - IGP (originated in the AS) e - EGP (learned through EGP) ? - incomplete (learned by other means)	
Network	Destination network address	
PrefixLen	Prefix length	
NextHop	Next Hop	
MED	MULTI_EXIT_DISC attribute	
LocPrf	Local preference value	
Path	AS_PATH attribute, recording the ASs the packet has passed to avoid routing loops	
PrefVal	Preferred value	
Label	Label	
Ogn	Origin attribute of the route, which can take on one of the following values:	
	i	Indicates that a route is interior to the AS. Summary routes and the routes configured using the **network** command are considered IGP routes.
	e	Indicates that a route is learned from the exterior gateway protocol (EGP).
	?	Short for INCOMPLETE. It indicates that the origin of a route is unknown and the route is learned by other means. BGP sets Origin attribute of routes learned from other IGP protocols to INCOMPLETE.

display bgp ipv6 routing-table as-path-acl

Syntax **display bgp ipv6 routing-table as-path-acl** *as-path-acl-number*

View Any view

Parameters *as-path-acl-number*: Number of an AS path ACL permitted by which to display routing information, ranging from 1 to 256.

Description Use the **display bgp ipv6 routing-table as-path-acl** command to display routes filtered through the specified AS path ACL.

Examples # Display routes filtered through the AS path ACL 20.

```
<Sysname> display bgp ipv6 routing-table as-path-acl 20
 BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table community

Syntax **display bgp ipv6 routing-table community** [*aa:nn*&<1-13>] [**no-advertise** | **no-export** | **no-export-subconfed**] * [**whole-match**]

View Any view

Parameters *aa:nn*: Specifies a community number; both aa and nn are in the range 0 to 65535.

&<1-13>: Indicates the argument before it can be entered up to 13 times.

no-advertise: Displays routes not advertised to any peer.

no-export: Displays routes advertised outside the AS; if there is a confederation, it displays routes not advertised outside the confederation, but to other sub ASs in the confederation.

no-export-subconfed: Displays routes neither advertised outside the AS nor to other sub ASs if the confederation is configured.

whole-match: Displays the exactly matched routes.

Description Use the **display bgp ipv6 routing-table community** command to display the routing information of the specified community.

Examples # Display the routing information of the community no-export.

```
<Sysname> display bgp ipv6 routing-table community no-export
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                          Label     : NULL
     MED     : 0
     Path/Ogn: i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table community-list

Syntax **display bgp ipv6 routing-table community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16>

View Any view

Parameters *basic-community-list-number*: Specifies a basic community-list number, in the range 1 to 99.

adv-community-list-number: Specifies an advanced community-list number, in the range 100 to 199.

whole-match: Displays routes exactly matching the specified *basic-community-list-number*.

&<1-16>: Specifies to allow entering the argument before it up to 16 times.

Description Use the **display bgp ipv6 routing-table community-list** command to view the routing information matching the specified IPv6 BGP community list.

Examples # Display the routing information matching the specified IPv6 BGP community list.

```
<Sysname> display bgp ipv6 routing-table community-list 99
BGP Local router ID is 30.30.30.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 30:30::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                          Label     : NULL
     MED      : 0
     Path/Ogn: i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table dampened

Syntax **display bgp ipv6 routing-table dampened**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table dampened** command to display the IPv6 BGP dampened routes.

Examples # Display IPv6 BGP dampened routes.

```
<Sysname> display bgp ipv6 routing-table dampened
```

```
BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network : 111::                                  PrefixLen : 64
     From    : 122::1                                    Reuse     : 00:29:34
     Path/Ogn: 200?
```

Table 292 Description on the fields of the display bgp ipv6 routing-table dampened command

Field	Description
From	Source IP address of a route
Reuse	Time for reuse

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table dampening parameter

Syntax **display bgp ipv6 routing-table dampening parameter**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table dampening parameter** command to display IPv6 BGP routing dampening parameters.

Related commands: **dampening (IPv6 address family view)**.

Examples # Display IPv6 BGP routing dampening parameters.

```
<Sysname> display bgp ipv6 routing-table dampening parameter
 Maximum Suppress Time(in second)     : 3069
 Ceiling Value                        : 16000
 Reuse Value                          : 750
 HalfLife Time(in  second)            : 900
 Suppress-Limit                       : 2000
```

Table 293 Description on the above fields

Field	Description
Maximum Suppress Time	Maximum Suppress Time
Ceiling Value	Upper limit of penalty value
Reuse Value	Reuse Value
HalfLife Time	Half life Time
Suppress-Limit	Suppress value

display bgp ipv6 routing-table different-origin-as

Syntax **display bgp ipv6 routing-table different-origin-as**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table different-origin-as** command to display IPv6 BGP routes originating from different autonomous systems.

Examples # Display IPv6 BGP routes from different ASs.

```
<Sysname> display bgp ipv6 routing-table different-origin-as


 BGP Local router ID is 10.1.4.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 100::                                    PrefixLen : 64
     NextHop : 1::1                                     LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: 100 i

 *   Network : 100::                                    PrefixLen : 64
     NextHop : 2::1                                     LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: 300 i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table flap-info

Syntax **display bgp ipv6 routing-table flap-info** [**regular-expression** *as-regular-expression* | **as-path-acl** *as-path-acl-number* | *ipv6-address* [*prefix-length* [**longer-match**]]]

View Any view

Parameters *as-regular-expression*: AS path regular expression to be matched.

as-path-acl-number: Number of the specified AS path ACL to be matched, ranging from 1 to 256.

ipv6-address: IPv6 address of a route to be displayed.

prefix-length: Prefix length of the IPv6 address, in the range 1 to 128.

longer-match: Matches the longest prefix.

Description Use the **display bgp ipv6 routing-table flap-info** command to display IPv6 BGP route flap statistics.

Examples # Display IPv6 BGP route flap statistics.

```
<Sysname> display bgp ipv6 routing-table flap-info

 BGP Local router ID is 1.1.1.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *d  Network  : 111::                                PrefixLen : 64
     From     : 122::1                               Flaps     : 3
     Duration : 00:13:47                             Reuse     : 00:16:36
     Path/Ogn : 200?
```

Table 294 Description on the fields of the display bgp ipv6 routing-table flap-info command

Field	Description
Flaps	Number of flaps
Duration	Flap duration
Reuse	Reuse time of the route

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table label

Syntax **display bgp ipv6 routing-table label**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table label** command to display IPv6 BGP label routing information.

Examples # Display IPv6 BGP label routing information.

```
<Sysname> display bgp ipv6 routing-table label
Total Number of Routes: 1

  Network              Prefix   NextHop                Label

  200::                96       ::FFFF:2.1.1.1         NULL/1024
```

Table 295 Description on the fields of the display bgp ipv6 routing-table label command

Field	Description
Network	Network address
Prefix	Prefix length
NextHop	Next hop
Label	MPLS label information

display bgp ipv6 routing-table peer

Syntax **display bgp ipv6 routing-table peer** { *ipv4-address* | *ipv6-address* } { **advertised-routes** | **received-routes** } [*network-address prefix-length* | **statistic**]

View Any view

Parameters *ipv4-address:* Specifies the IPv4 peer to be displayed.

ipv6-address: Specifies the IPv6 peer to be displayed.

advertised-routes: Routing information advertised to the specified peer.

received-routes: Routing information received from the specified peer.

network-address prefix-length: IPv6 address and prefix length. The prefix length ranges from 0 to 128.

statistic: Displays route statistics.

Description Use the **display bgp ipv6 routing-table peer** command to display the routing information advertised to or received from the specified IPv4 or IPv6 BGP peer.

Examples # Display the routing information advertised to the specified BGP peer.

```
<Sysname> display bgp ipv6 routing-table peer 10:10::10:1 advertised-routes
 Total Number of Routes: 2

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 20:20::                                  PrefixLen : 64
     NextHop : 20:20::20:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL
     MED     : 0
     Path/Ogn: i

 *>  Network : 40:40::                                  PrefixLen : 64
     NextHop : 30:30::30:1                              LocPrf    :
     PrefVal : 0                                        Label     : NULL

     MED     : 0
     Path/Ogn: 300 i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table regular-expression

Syntax **display bgp ipv6 routing-table regular-expression** *as-regular-expression*

View Any view

Parameters *as-regular-expression*: AS regular expression.

Description Use the **display bgp ipv6 routing-table regular-expression** command to display the routes permitted by the specified AS regular expression.

Examples # Display routing information matching the specified AS regular expression.

```
<Sysname> display bgp ipv6 routing-table regular-expression ^100

 BGP Local router ID is 20.20.20.1
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 *>  Network : 50:50::                                  PrefixLen : 64
     NextHop : 10:10::10:1                             LocPrf    :
     PrefVal : 0                                       Label     : NULL
     MED     : 0
     Path/Ogn: 100 i
```

Refer to Table 291 for description on the fields above.

display bgp ipv6 routing-table statistic

Syntax **display bgp ipv6 routing-table statistic**

View Any view

Parameters None

Description Use the **display bgp ipv6 routing-table statistic** command to display IPv6 BGP routing statistics.

Examples # Display IPv6 BGP routing statistics.

```
<Sysname> display bgp ipv6 routing-table statistic
 Total Number of Routes: 1
```

filter-policy export(IPv6 address family view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol process-id*]

undo filter-policy export [*protocol process-id*]

View IPv6 address family view

Parameters *acl6-number*: Specifies the number of an ACL6 used to match against the destination of routing information. The number is in the range 2000 to 3999.

ipv6-prefix-name: Specifies the name of an IPv6 prefix list used to match against the destination address field of routing information. The name is a string of 1 to 19 characters.

protocol: Filters routes redistributed from the routing protocol. It can be **direct**, **isisv6**, **ospfv3**, **ripng**, and **static** at present. If no protocol is specified, all routes will be filtered when advertised.

process-id: Process ID of the routing protocol, in the range 1 to 65535. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description Use the **filter-policy export** command to filter outbound routes using a specified filter.

Use the **undo filter-policy export** command to cancel filtering outbound routes.

By default, no outbound routing information is filtered.

If a protocol is specified, only routes redistributed from the specified protocol are filtered. If no protocol is specified, all redistributed routes will be filtered.

Examples # Reference ACL6 2001 to filter all outbound IPv6 BGP routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 export
```

filter-policy import (IPv6 address family view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View IPv6 address family view

Parameters *acl6-number*: Number of an IPv6 ACL used to match against the destination address field of routing information, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to match against the destination address field of routing information, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to filter inbound routing information using a specified filter.

Use the **undo filter-policy import** command to cancel filtering inbound routing information.

By default, no inbound routing information is filtered.

Examples # Reference ACL6 2001 to filter all inbound routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] filter-policy 2001 import
```

group (IPv6 address family view)

Syntax **group** *ipv6-group-name* [**internal** | **external**]

undo group *ipv6-group-name*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of an IPv6 peer group, a string of 1 to 47 characters.

internal: Creates an IBGP peer group.

external: Creates an EBGP peer group, which can be a group of another sub AS in the confederation.

Description Use the **group** command to create a peer group.

Use the **undo group** command to delete a peer group.

An IBGP peer group will be created if neither **internal** nor **external** is selected.

Examples # Create an IBGP peer group named **test**.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv6-family
[Sysname-bgp-af-ipv6] group test
```

import-route (IPv6 address family view)

Syntax **import-route** *protocol* [*process-id* [**med** *med-value* | **route-policy** *route-policy-name*] *]

undo import-route *protocol* [*process-id*]

View IPv6 address family view

Parameters *protocol*: Redistributes routes from the specified protocol, which can be **direct**, **isisv6**, **ospfv3**, **ripng**, or **static** at present.

process-id: Process ID, in the range 1 to 65535. The default is 1. It is available only when the protocol is **isisv6**, **ospfv3** or **ripng**.

med-value: Applies the MED value to redistributed routes. The value is in the range 0 to 4294967295. If not specified, the cost of the redistributed route is used as its MED in the IPv6 BGP routing domain.

route-policy-name: Name of a routing policy used to filter redistributed routes, a string of 1 to 19 characters.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to remove the configuration.

By default, IPv6 BGP does not redistribute routes from any routing protocol.

The routes redistributed using the **import-route** command has the incomplete origin attribute.

Examples # Redistribute routes from RIPng 1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] import-route ripng 1
```

ipv6-family

Syntax **ipv6-family**

undo ipv6-family

View BGP view

Parameters None

Description Use the **ipv6-family** command to enter IPv6 address family view.

Use the **undo ipv6-family** command to remove all configurations from the view.

IPv4 BGP unicast view is the default.

Examples # Enter IPv6 address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
```

network (IPv6 address family view)

Syntax **network** *ipv6-address prefix-length* [**short-cut** | **route-policy** *route-policy-name*]

undo network *ipv6-address prefix-length* [**short-cut**]

View IPv6 address family view

Parameters *ipv6-address*: IPv6 address.

prefix-length: Prefix length of the address, in the range 0 to 128.

short-cut: If the keyword is specified for an EBGP route, the route will use the local routing management value rather than that of EBGP routes, so the preference of the route is reduced.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description Use the **network** command to advertise a network to the IPv6 BGP routing table.

Use the **undo network** command to remove an entry from the IPv6 BGP routing table.

By default, no route is advertised.

Note that:

- The route to be advertised must exist in the local IP routing table, and using a routing policy makes route management more flexible.
- The route advertised to the BGP routing table using the **network** command has the IGP origin attribute.

Examples # Advertise the network 2002::/16 into the IPv6 BGP routing table.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] network 2002:: 16
```

peer advertise-community (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-community**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-community** command to advertise the community attribute to a peer/peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attribute is advertised to any peer group/peer.

Examples # Advertise the community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-community
```

peer advertise-ext-community (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **advertise-ext-community**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **peer advertise-ext-community** command to advertise the extended community attribute to a peer/peer group.

Use the **undo peer advertise-ext-community** command to remove the configuration.

By default, no extended community attribute is advertised to a peer/peer group.

Examples # Advertise the extended community attribute to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 advertise-ext-community
```

peer allow-as-loop (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **allow-as-loop**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

number: Specifies the repeating times of the local AS number, in the range 1 to 10. The default number is 1.

Description Use the **peer allow-as-loop** command to configure IPv6 BGP to allow the local AS number to exist in the AS_PATH attribute of routes from a peer/peer group, and to configure the repeating times of the local AS number.

Use the **undo peer allow-as-loop** command to disable the function.

The local AS number is not allowed to exist in the AS PATH attribute of routes by default.

Examples # Configure the repeating times of the local AS number allowed in the AS PATH of routes from peer 1::1 as 2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1::1 allow-as-loop 2
```

peer as-number (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **as-number** *as-number*

undo peer *ipv6-group-name* **as-number**

undo peer *ipv6-address*

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: AS number of the peer/peer group, in the range 1 to 65535.

Description Use the **peer as-number** command to specify an AS number for a peer/peer group.

Use the **undo peer as-number** command to delete the AS number of a peer group.

Use the **undo peer** command to delete a peer.

By default, no AS number is configured for a peer/peer group.

Examples # Specify the AS number of the peer group test as 100.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test as-number 100
```

peer as-path-acl (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **as-path-acl** *as-path-acl-number* { **import** | **export** }

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-path-acl-number: Number of an AS path ACL, in the range 1 to 256.

import: Filters incoming routes.

export: Filters outgoing routes.

Description Use the **peer as-path-acl** command to specify an AS path ACL to filter routes incoming from or outgoing to a peer/peer group.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS path list is specified for filtering.

Examples # Specify the AS path ACL 3 to filter routes outgoing to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip as-path-acl 3 permit ^200
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-path-acl 3 export
```

peer capability-advertise route-refresh

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

undo peer { *ipv6-group-name* | *ipv6-address* } **capability-advertise route-refresh**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer capability-advertise route-refresh** command to enable IPv6 BGP route-refresh.

Use the **undo peer capability-advertise route-refresh** command to disable the function.

By default, route-refresh is enabled.

Examples # Disable route-refresh of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] undo peer 1:2::3:4 capability-advertise route-refresh
```

peer connect-interface (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **connect-interface** *interface-type interface-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **connect-interface**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

interface-type interface-number: Specifies the type and name of the interface.

Description Use the **peer connect-interface** command to specify the source interface for establishing TCP connections to an IPv6 BGP peer or peer group.

Use the **undo peer connect-interface** command to restore the default.

By default, BGP uses the outbound interface of the best route to the IPv6 BGP peer/peer group as the source interface for establishing a TCP connection.

Note that:

To establish multiple BGP connections to a BGP router, you need to specify on the local router the respective source interfaces for establishing TCP connections to the peers on the peering BGP router; otherwise, the local BGP router may fail to establish TCP connections to the peers when using the outbound interfaces of the best routes as the source interfaces.

Examples # Specify loopback0 as the source interface for routing updates to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 connect-interface loopback 0
```

peer default-route-advertise

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise** [**route-policy** *route-policy-name*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **default-route-advertise**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Route-policy name, a string of 1 to 19 characters.

Description Use the **peer default-route-advertise** command to advertise a default route to a peer/peer group.

Use the **undo peer default-route-advertise** command to disable advertising a default route.

By default, no default route is advertised to a peer/peer group.

Using this command does not require the default route available in the routing table. With this command used, the router sends the default route unconditionally to the peer/peer group with the next hop being itself.

Examples # Advertise a default route to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 default-route-advertise
```

peer description (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **description** *description-text*

undo peer { *ipv6-group-name* | *ipv6-address* } **description**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

description-text: Description information for the peer/peer group, a string of 1 to 79 characters.

Description Use the **peer description** command to configure the description information for a peer/peer group.

Use the **undo peer description** command to remove the description information of a peer/peer group.

By default, no description information is configured for a peer (group).

You need create a peer/peer group before configuring a description for it.

Examples # Configure the description for the peer group **test** as ISP1.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test description ISP1
```

peer ebgp-max-hop (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop** [*hop-count*]

undo peer { *ipv6-group-name* | *ipv6-address* } **ebgp-max-hop**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

hop-count: Maximum hop count, in the range 1 to 255. By default, the value is 64.

Description Use the **peer ebgp-max-hop** command to allow establishing the EBGP connection to a peer/peer group indirectly connected.

Use the **undo peer ebgp-max-hop** command to remove the configuration.

By default, this feature is disabled.

You can use the argument *hop-count* to specify the maximum router hops of the EBGP connection.

Examples # Allow establishing the EBGP connection with the peer group **test** on an indirectly connected network.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test ebgp-max-hop
```

peer enable (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* } **enable**

undo peer { *group-name* | *ipv4-address* } **enable**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 peer group, a string of 1 to 47 characters. The IPv4 peer group should be created beforehand.

ipv4-address: IPv4 address of a peer.

Description Use the **peer enable** command to enable an IPv4 peer or peer group.

Use the **undo peer enable** command to disable an IPv4 peer or peer group.

By default, no IPv4 peer or peer group is enabled.

If an IPv4 peer or peer group is disabled, the router will not exchange routing information with it.

Examples # Enable peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1.1.1.1 enable
```

peer fake-as (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **fake-as** *as-number*

undo peer { *ipv6-group-name* | *ipv6-address* } **fake-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

as-number: Local autonomous system number, in the range 1 to 65535.

Description Use the **peer fake-as** command to configure a fake local AS number for a peer or peer group.

Use the **undo peer fake-as** command to remove the configuration.

By default, no fake local AS number is configured for a peer or peer group.

Examples # Configure a fake AS number of 200 for the peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test fake-as 200
```

peer filter-policy (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** *acl6-number* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **filter-policy** [*acl6-number*] { **import** | **export** }

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

acl6-number: IPv6 ACL number, in the range 2000 to 3999.

import: Applies the filter-policy to routes received from the peer/peer group.

export: Applies the filter-policy to routes advertised to the peer/peer group.

Description Use the **peer filter-policy** command to configure an ACL-based filter policy for a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no ACL-based filter policy is configured for a peer or peer group.

Examples # Apply the ACL6 2000 to filter routes advertised to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 filter-policy 2000 export
```

peer group (IPv6 address family view)

Syntax **peer** { *ipv4-address* | *ipv6-address* } **group** *group-name* [**as-number** *as-number*]

undo peer *ipv6-address* **group** *group-name*

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

as-number: Specifies the AS number of the peer/peer group, in the range 1 to 65535.

Description Use the **peer group** command to add a peer to a configured peer group.

Use the **undo peer group** command to delete a specified peer from a peer group.

By default, the peer does not belong to any peer group.

Examples # Create a peer group named **test** and add the peer 1:2::3:4 to the peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 200
[Sysname-bgp-af-ipv6] peer 1:2::3:4 group test
```

peer ignore (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **ignore**

undo peer { *ipv6-group-name* | *ipv6-address* } **ignore**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer ignore** command to terminate the session to a peer or peer group.

Use the **undo peer ignore** command to remove the configuration.

By default, a router can establish sessions with a peer or peer group.

After the **peer ignore** command is executed, the system terminates the active session(s) with the specified peer or peer group and clears all the related routing information. For a peer group, this means all the sessions with the peer group will be tore down.

Examples # Terminate the session with peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ignore
```

peer ipv6-prefix

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** *ipv6-prefix-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **ipv6-prefix** { **import** | **export** }

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

ipv6-prefix-name: IPv6 prefix list name, a string of 1 to 19 characters.

import: Applies the filtering policy to routes received from the specified peer/peer group.

export: Applies the filtering policy to routes advertised to the specified peer/peer group.

Description Use the **peer ipv6-prefix** command to specify an IPv6 prefix list to filter routes incoming from or outgoing to a peer or peer group.

Use the **undo peer ipv6-prefix** command to remove the configuration.

By default, no IPv6 prefix list is specified for filtering.

Examples # Reference the IPv6 prefix list **list 1** to filter routes outgoing to peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix list1 permit 2002:: 64
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 ipv6-prefix list1 export
```

peer keep-all-routes (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **keep-all-routes**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **peer keep-all-routes** command to save the original routing information from a peer or peer group, including even routes that failed to pass the inbound policy.

Use the **undo peer keep-all-routes** command to disable this function.

By default, the function is not enabled.

Examples # Save routing information from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 keep-all-routes
```

peer label-route-capability (IPv6 address family view)

Syntax **peer** *ipv4-address* **label-route-capability**

undo peer *ipv4-address* **label-route-capability**

View IPv6 address family view

Parameters *ipv4-address*: IPv4 address of a peer.

Description Use the **peer label-route-capability** command to enable exchange of labeled IPv4 routes with the peer.

Use the **undo peer label-route-capability** command to disable exchange of labeled IPv4 routes with the peer.

By default, the feature is disabled.

Examples # Enable exchange of labeled IPv4 routes with peer 2.2.2.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 2.2.2.2 label-route-capability
```

peer log-change (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **log-change**

undo peer { *ipv6-group-name* | *ipv6-address* } **log-change**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer log-change** command to enable the logging of session state and event information of a specified peer or peer group.

Use the **undo peer log-change** command to remove the configuration.

The logging is enabled by default.

Examples # Enable the logging of session state and event information of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 log-change
```

peer next-hop-local (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

undo peer { *ipv6-group-name* | *ipv6-address* } **next-hop-local**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer next-hop-local** command to configure the next hop of routes advertised to a peer/peer group as the local router.

Use the **undo peer next-hop-local** command to restore the default.

By default, the system sets the next hop of routes advertised to an EBGP peer/peer group to the local router, but does not set for routes outgoing to an IBGP peer/peer group.

Examples # Set the next hop of routes advertised to EBGP peer group **test** to the router itself.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test next-hop-local
```

peer preferred-value (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value*

undo peer { *ipv6-group-name* | *ipv6-address* } **preferred-value**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

value: Preferred value, in the range 0 to 65535.

Description Use the **peer preferred-value** command to assign a preferred value to routes received from a peer or peer group.

Use the **undo peer preferred-value** command to restore the default.

By default, routes received from a peer or peer group have a preferred value of 0.

Routes learned from peers each have an initial preferred value. Among multiple routes to the same destination, the route with the biggest value is selected.

Note that:

If you both reference a routing policy and use the command **peer** { *ipv6-group-name* | *ipv6-address* } **preferred-value** *value* to set a preferred value for routes from a peer, the routing policy sets a non-zero preferred value for routes matching it. Other routes not matching the routing policy uses the value set with the command. If the preferred value in the routing policy is zero, the routes matching it will also use the value set with the command. For information about using a routing policy to set a preferred value, refer to "peer group (IPv6 address family view)" on page 1251 and **"peer route-policy (IPv6 address family view)" on page 1258** { **import** | **export** } in this document and "apply preferred-value" on page 1194.

Examples # Configure the preferred value as 50 for routes from peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 preferred-value 50
```

peer public-as-only (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **public-as-only**

undo peer { *ipv6-group-name* | *ipv6-address* } **public-as-only**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer public-as-only** command to configure IPv6 BGP updates to a peer/peer group to not carry private AS numbers.

Use the **undo peer public-as-only** command to allow IPv6 BGP updates to a peer/peer group to carry private AS numbers.

By default, BGP updates carry the private AS number.

The command does not take effect if the BGP update has both the public AS number and private AS number. The range of private AS number is from 64512 to 65535.

Examples # Carry no private AS number in BGP updates sent to the peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 public-as-only
```

peer reflect-client (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **reflect-client**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

Description Use the **peer reflect-client** command to configure the router as a route reflector and specify a peer/peer group as a client.

Use the **undo peer reflect-client** command to remove the configuration.

By default, neither route reflector nor client is configured.

Related commands: **reflect between-clients (IPv6 address family view)** and **reflector cluster-id (IPv6 address family view)**.

Examples # Configure the local device as a route reflector and specify the peer group **test** as a client.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test
[Sysname-bgp-af-ipv6] peer test reflect-client
```

peer route-limit (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit** *limit* [*percentage*]

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-limit**

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

limit: Specifies an upper limit from 1 to 10000 for address prefixes that can be received from the peer or peer group

percentage: Specifies the percentage of routes to generate alarm information, ranging from 1 to 100, with the default as 75.

Description Use the **peer route-limit** command to set the maximum number of prefixes that can be received from a peer/peer group.

Use the **undo peer route-limit** command to restore the default.

By default, the router has no limit on prefixes from a peer/peer group.

The router will end the peer relation when the number of address prefixes received for the peer exceeds the limit.

Examples # Set the number of prefixes allowed to receive from the peer 1:2::3:4 to 10000.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-limit 10000
```

peer route-policy (IPv6 address family view)

Syntax **peer** { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

undo peer { *group-name* | *ipv4-address* | *ipv6-address* } **route-policy** *route-policy-name* { **import** | **export** }

View IPv6 address family view

Parameters *group-name*: Name of an IPv4 or IPv6 peer group, a string of 1 to 47 characters.

ipv4-address: IPv4 address of a peer.

ipv6-address: IPv6 address of a peer.

route-policy-name: Specifies route-policy name, a string of 1 to 19 characters.

import: Applies the routing policy to routes from the peer (group).

export: Applies the routing policy to routes to the peer (group).

Description Use the **peer route-policy** command to apply a routing policy to routes incoming from or outgoing to a peer or peer group.

Use the **undo peer route-policy** command to remove the configuration.

By default, no routing policy is specified for the peer (group).

Use of the **peer route-policy** command does not apply the **if-match interface** clause defined in the routing policy. Refer to ***if-match interface*** on page 1200.

Examples # Apply the routing policy test-policy to routes received from the peer group test.

```
<Sysname> system-view
[Sysname] route-policy test-policy permit node 10
[Sysname-route-policy] if-match cost 10
[Sysname-route-policy] apply cost 65535
[Sysname-route-policy] quit
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test route-policy test-policy import
```

peer route-update-interval (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **route-update-interval** *seconds*

undo peer { *ipv6-group-name* | *ipv6-address* } **route-update-interval**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

seconds: Specifies the minimum interval for sending the same update to a peer (group) from 5 to 600 seconds.

Description Use the **peer route-update-interval** command to specify the interval for sending the same update to a peer/peer group.

Use the **undo peer route-update-interval** command to restore the default.

By default, the interval is 15 seconds for the IBGP peer, and 30 seconds for the EBGP peer.

Examples # Specify the interval for sending the same update to the peer 1:2::3:4 as 10 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 as-number 100
[Sysname-bgp-af-ipv6] peer 1:2::3:4 route-update-interval 10
```

peer substitute-as (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **substitute-as**

undo peer { *ipv6-group-name* | *ipv6-address* } **substitute-as**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

Description Use the **peer substitute-as** command to substitute the local AS number for the AS number of a peer/peer group in the AS_PATH attribute.

Use the **undo peer substitute-as** command to remove the configuration.

The substitution is not configured by default.

Examples # Substitute the local AS number for the AS number of peer 1:2::3:4.

```
<Sysname> system-view
[Sysname] bgp 100
```

```
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] peer 1:2::3:4 substitute-as
```

peer timer (IPv6 address family view)

Syntax **peer** { *ipv6-group-name* | *ipv6-address* } **timer keepalive** *keepalive* **hold** *holdtime*

undo peer { *ipv6-group-name* | *ipv6-address* } **timer**

View IPv6 address family view

Parameters *ipv6-group-name*: Name of a peer group, a string of 1 to 47 characters.

ipv6-address: IPv6 address of a peer.

keepalive: Specifies the keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Specifies the holdtime in seconds, ranging from 3 to 65535.

Description Use the **peer timer** command to configure keepalive interval and holdtime interval for a peer or peer group.

Use the **undo peer timer** command to restore the default.

keepalive interval defaults to 60 seconds, and *holdtime* interval defaults to 180 seconds

Note that:

- The timer configured with this command is preferred to the timer configured with the **timer** command.
- The holdtime interval must be at least three times the keepalive interval.

Related commands: **timer (IPv6 address family view)**.

Examples # Configure the keepalive interval and holdtime interval for the peer group test as 60 seconds and 180 seconds.

```
<Sysname] system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] group test external
[Sysname-bgp-af-ipv6] peer test timer keep-alive 60 hold 180
```

preference (IPv6 address family view)

Syntax **preference** { *external-preference internal-preference local-preference* | **route-policy** *route-policy-name* }

undo preference

View IPv6 address family view

Parameters *external-preference*: Preference of EBGP route learned from an EBGP peer, in the range 1 to 255.

internal-preference: Preference of IBGP route learned from an IBGP peer, in the range 1 to 255.

local-preference: Preference of IPv6 BGP local route, in the range 1 to 255.

route-policy-name: Routing policy name, a string of 1 to 19 characters. The routing policy can set a preference for routes passing it. To the routes filtered out, the default value applies.

Description Use the **preference** command to configure preferences for EBGP, IBGP, and local routes.

Use the **undo preference** command to restore the default.

The bigger the preference value is, the lower the preference is. The default values of *external-preference*, *internal-preference* and *local-preference* are 255, 255 and 130 respectively.

Examples # Configure preferences for EBGP, IBGP, and local routes as 20, 20 and 200.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] preference 20 20 200
```

reflect between-clients (IPv6 address family view)

Syntax **reflect between-clients**

undo reflect between-clients

View IPv6 address family view

Parameters None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable this function.

By default, route reflection between clients is enabled.

After a route reflector is configured, it reflects routes between clients. If the clients are fully meshed, it is recommended to disable route reflection on the route reflector to reduce costs.

Related commands: **reflector cluster-id (IPv6 address family view)** and **peer reflect-client (IPv6 address family view)**.

Examples # Enable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflect between-clients
```

reflector cluster-id (IPv6 address family view)

Syntax **reflector cluster-id** *cluster-id*

undo reflector cluster-id

View IPv6 address family view

Parameters *cluster-id*: Specifies the cluster ID of the route reflector, an integer from 1 to 4294967295 (the system translates it into an IPv4 address) or an IPv4 address.

Description Use the **reflector cluster-id** command to configure the cluster ID of the route reflector.

Use the **undo reflector cluster-id** command to remove the configured cluster ID.

By default, a route reflector uses its router ID as the cluster ID.

Usually, there is only one route reflector in a cluster, so the router ID of the route reflector identifies the cluster. If multiple route reflectors are configured to improve the stability of the network, you should use this command to configure the identical cluster ID for all the reflectors to avoid routing loops.

Related commands: **reflect between-clients (IPv6 address family view)** and **peer reflect-client (IPv6 address family view)**.

Examples # Set 50 as the cluster ID for the route reflector, which is one of multiple route reflectors in the cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] reflector cluster-id 50
```

refresh bgp ipv6

Syntax **refresh bgp ipv6** { *ipv4-address* | *ipv6-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** }

View User view

Parameters *ipv4-address*: Soft-resets the connection with an IPv4 BGP peer.

ipv6-address: Soft-resets the connection with an IPv6 BGP peer.

all: Soft-resets all IPv6 BGP connections.

external: Soft-resets EBGP connections.

group *ipv6-group-name*: Soft-resets connections with a peer group. The name of the peer group is a string of 1 to 47 characters.

internal: Soft-resets IBGP connections.

export: Performs soft reset in outbound direction.

import: Performs soft reset in inbound direction.

Description Use the **refresh bgp ipv6** command to soft reset specified IPv4/IPv6 BGP connections. With this feature, you can refresh the IPv4/IPv6 BGP routing table and apply a new available policy without tearing down IPv4/IPv6 BGP connections.

To perform IPv4/IPv6 BGP soft reset, all routers in the network should support route-refresh. If a router not supporting route refresh exists in the network, you need to use the **peer keep-all-routes** command on the local router to save all route updates before performing soft reset.

Examples # Soft reset inbound IPv6 BGP connections.

```
<Sysname> refresh bgp ipv6 all import
```

reset bgp ipv6

Syntax **reset bgp ipv6** { *as-number* | *ipv4-address* | *ipv6-address* [**flap-info**] | **all** | **group** *group-name* | **external** | **internal** }

View User view

Parameters *as-number*: Resets the IPv6 BGP connections to peers in the specified AS.

ipv4-address: Resets the connection to the specified IPv4 BGP peer.

ipv6-address: Resets the connection to the specified IPv6 BGP peer.

flap-info: Clears the history information of routing flaps.

all: Resets all IPv6 BGP connections.

group *group-name*: Resets the connections to the specified IPv6 BGP peer group.

external: Resets all the EBGP connections.

internal: Resets all the IBGP connections.

Description Use the **reset bgp ipv6** command to reset specified IPv4/IPv6 BGP connections.

Examples # Reset all the IPv6 BGP connections.

```
<Sysname> reset bgp ipv6 all
```

reset bgp ipv6 dampening

Syntax **reset bgp ipv6 dampening** [*ipv6-address prefix-length*]

View User view

Parameters *ipv6-address*: IPv6 address

prefix-length: Prefix length of the address, in the range 0 to 128.

Description Use the **reset bgp ipv6 dampening** command to clear route dampening information and release suppressed routes.

If no *ipv6-address prefix-length* is specified, all IPv6 route dampening information will be cleared.

Examples # Clear the damping information of routes to 2345::/64 and release suppressed routes.

```
<Sysname> reset bgp ipv6 dampening 2345:: 64
```

reset bgp ipv6 flap-info

Syntax **reset bgp ipv6 flap-info** [*ipv6-address/prefix-length* | **regexp** *as-path-regexp* | **as-path-acl** *as-path-acl-number*]

View User view

Parameters *ipv6-address*: Clears the flap statistics for the specified IPv6 address.

prefix-length: Prefix length of the address, in the range 1 to 128.

as-path-regexp: Clears the flap statistics for routes matching the AS path regular expression.

as-path-acl-number: Clears the flap statistics for routes matching the AS path ACL. The number is in the range 1 to 256.

Description Use the **reset bgp ipv6 flap-info** command to clear IPv6 routing flap statistics.

If no parameters are specified, the flap statistics of all the routes will be cleared

Examples # Clear the flap statistics of the routes matching AS path ACL 10.

```
<Sysname> system-view
[Sysname] ip as-path-acl 10 permit ^100.*200$
[Sysname] quit
<Sysname> reset bgp ipv6 flap-info as-path-acl 10
```

router-id

Syntax **router-id** *router-id*

undo router-id

View BGP view

Parameters *router-id*: Router ID in IP address format.

Description Use the **router-id** command to specify a router ID for the router.

Use the **undo router-id** command to remove a router ID.

To run IPv6 BGP protocol, a router must have a router ID, an unsigned 32-bit integer and the unique ID of the router in the AS.

A router ID can be configured manually. If not, the system will select a router ID automatically from the current interfaces' IPv4 addresses. The selection sequence is the highest IPv4 address of Loopback interfaces' addresses, then the highest IPv4 address of physical interfaces' addresses if no Loopback interfaces are configured.

Only when the interface with the router ID is removed or the manually configured router ID is removed, will the system select another Router ID. To improve network reliability, it is recommended to configure the IPv4 address of a loopback interface as the router ID.

Examples # Specify the router ID of the router as 10.18.4.221.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] router-id 10.18.4.221
```

synchronization (IPv6 address family view)

Syntax **synchronization**

undo synchronization

View IPv6 address family view

Parameters None

Description Use the **synchronization** command to enable the synchronization between IPv6 BGP and IGP.

Use the **undo synchronization** command to disable the synchronization.

The feature is disabled by default.

With this feature enabled and when a non-BGP router is responsible for forwarding packets in an AS, IPv6 BGP speakers in the AS cannot advertise routing information to other ASs unless all routers in the AS know the latest routing information.

By default, upon receiving an IPv6 IBGP route, the BGP router only checks whether the next hop is reachable before advertisement. If synchronization is enabled, the IBGP route can be advertised to EBGP peers only when the route is also advertised by the IGP.

Examples # Enable the route synchronization between IPv6 BGP and IGP.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] synchronization
```

timer (IPv6 address family view)

Syntax **timer keepalive** *keepalive* **hold** *holdtime*

undo timer

View IPv6 address family view

Parameters *keepalive*: Keepalive interval in seconds, ranging from 1 to 21845.

holdtime: Holdtime interval in seconds, ranging from 3 to 65535.

Description Use the **timer** command to specify IPv6 BGP keepalive interval and holdtime interval.

Use the **undo timer** command to restore the default.

By default, the keepalive and holdtime intervals are 60s and 180s respectively.

Note that:

- Timer configured using the peer timer command is preferred to the timer configured using the timer command.
- The holdtime interval must be at least three times the keepalive interval.
- The configured timer applies to all the IPv6 BGP peers. It becomes valid only after the corresponding IPv6 BGP connections are reset.

Related commands: **peer timer (IPv6 address family view)**.

Examples # Configure keepalive interval and holdtime interval as 60 and 180 seconds.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv6-family
[Sysname-bgp-af-ipv6] timer keepalive 60 hold 180
```

83 IPv6 IS-IS CONFIGURATION COMMANDS

IPv6 IS-IS supports all the features of IPv4 IS-IS except that it advertises IPv6 routing information instead. This document describes only IPv6 IS-IS exclusive commands. Refer to "IS-IS Configuration Commands" on page 1037 for other IS-IS configuration commands.

display isis route ipv6

Syntax **display isis route ipv6** [[**level-1** | **level-2**] | **verbose**]* [*process-id*]

View Any view

Parameters **verbose**: Displays detailed IPv6 IS-IS routing information.

process-id: IS-IS process ID, in the range 1 to 65535.

level-1: Display Level-1 IPv6 IS-IS routes only.

level-2: Displays Level-2 IPv6 IS-IS routes only.

If no level is specified, both Level-1 and Level-2 (namely Level-1-2) routing information will be displayed.

Description Use the **display isis route ipv6** command to display IPv6 IS-IS routing information.

Examples # Display IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6
                        Route information for ISIS(1)
                        -----------------------------
                    ISIS(1) IPv6 Level-1 Forwarding Table
                    -------------------------------------
 Destination: 2001:1::                              PrefixLen: 64
 Flag       : R/L/-                                 Cost     : 20
 Next Hop   : FE80::200:5EFF:FE64:8905              Interface: Eth0/1/0
 Destination: 2001:2::                              PrefixLen: 64
 Flag       : D/L/-                                 Cost     : 10
 Next Hop   : Direct                                Interface: Eth0/1/0
   Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
                    ISIS(1) IPv6 Level-2 Forwarding Table
                    -------------------------------------
 Destination: 2001:1::                              PrefixLen: 64
 Flag       : -/-/-                                 Cost     : 20
 Destination: 2001:2::                              PrefixLen: 64
 Flag       : D/L/-                                 Cost     : 10
```

```
 Next Hop   : Direct                                    Interface: Eth0/1/0
   Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 296 Description on the fields of the display isis route ipv6 command

Field	Description
Destination	IPv6 destination address prefix
PrefixLen	Length of the prefix
Flag/Flags	Flag of routing information status
	D: Direct route
	R: The route has been added into the routing table.
	L: The route has been advertised in an LSP.
	U: Route leaking flag, indicating the Level-1 route is from Level-2. "UP" means the route will not be returned to Level-2.
Cost	Value of cost
Next Hop	Next hop
Interface	Outbound interface

Display detailed IPv6 IS-IS routing information.

```
<Sysname> display isis route ipv6 verbose
                        Route information for ISIS(1)
                        -----------------------------
                    ISIS(1) IPv6 Level-1 Forwarding Table
                    -------------------------------------
 IPV6 Dest  : 2001:1::/64                    Cost : 20            Flag : R/L/-
 Admin Tag  : -                          Src Count : 1
 NextHop    :                            Interface :          ExitIndex :
    FE80::200:5EFF:FE64:8905                 Eth0/1/0              0x00000003
 IPV6 Dest  : 2001:2::/64                    Cost : 10            Flag : D/L/-
 Admin Tag  : -                          Src Count : 2
 NextHop    :                            Interface :          ExitIndex :
    Direct                                   Eth0/1/0              0x00000000
   Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
                    ISIS(1) IPv6 Level-2 Forwarding Table
                    -------------------------------------
 IPV6 Dest  : 2001:1::/64                    Cost : 20            Flag : -/-/-
 Admin Tag  : -                          Src Count : 1
 IPV6 Dest  : 2001:2::/64                    Cost : 10            Flag : D/L/-
 Admin Tag  : -                          Src Count : 2
 NextHop    :                            Interface :          ExitIndex :
    Direct                                   Eth0/1/0              0x00000000
   Flags: D-Direct, R-Added to RM, L-Advertised in LSPs, U-Up/Down Bit Set
```

Table 297 Description on the fields of the display isis route ipv6 verbose command

Field	Description
IPV6 Dest	IPv6 destination address prefix
Cost	Value of cost
Flag/Flags	Flag of routing information status
	D: This is a direct route.
	R: The route has been added into the routing table.
	L: The route has been advertised in a LSP.
	U: Route leaking flag, indicating the Level-1 route is from Level-2. "UP" means the route will not be returned to Level-2.
Admin Tag	Administrative tag
Src Count	Number of advertisement sources
Next Hop	Next hop

Table 297 Description on the fields of the display isis route ipv6 verbose command

Field	Description
Interface	Outbound interface
ExitIndex	Outbound interface index

ipv6 default-route-advertise

Syntax **ipv6 default-route-advertise** [[**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name*]*

undo ipv6 default-route-advertise [**route-policy** *route-policy-name*]

View IS-IS view

Parameters *route-policy-name*: Specifies the name of a routing policy with a string of 1 to 19 characters.

level-1: Specifies the default route as Level-1.

level-2: Specifies the default route as Level-2.

level-1-2: Specifies the default route as Level-1-2.

If no level is specified, the default route belongs to Level-2.

Description Use the **ipv6 default-route-advertise** command to generate a Level-1 or Level-2 IPv6 IS-IS default route.

Use the **undo ipv6 default-route-advertise** command to disable generating a default route.

No IPv6 IS-IS default route is generated by default.

With a routing policy, you can configure IPv6 IS-IS to generate the default route that must match the routing policy. You can use the **apply isis level-1** command in routing policy view to generate a default route in L1 LSPs, or use the **apply isis level-2** command in routing policy view to generate a default route in L2 LSPs, and use the **apply isis level-1-2** in routing policy view to generate a default route in L1 and L2 LSPs respectively.

Refer to "apply isis" on page 1191 for information about the **apply isis** command.

Examples # Configure the router to generate a default route in Level-2 LSPs.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 default-route-advertise
```

ipv6 enable

Syntax **ipv6 enable**

undo ipv6 enable

View IS-IS view

Parameters None

Description Use the **ipv6 enable** command to enable IPv6 for the IPv6 IS-IS process.

Use the **undo ipv6 enable** command to disable IPv6.

IPv6 is disabled by default.

To run IPv6 IS-IS, you need enable global IPv6 capability, create an IS-IS process with the **isis** command, set a NET for the router with the **network-entity** command, then use the **ipv6 enable** command to enable IPv6 for the process, finally use the **isis ipv6 enable** command on relevant IS-IS interfaces to enable IPv6 for them.

Examples # Create IS-IS routing process 1, and enable IPv6 for the process.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
```

ipv6 filter-policy export

Syntax **ipv6 filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **export** [*protocol* [*process-id*]]

undo ipv6 filter-policy export [*protocol* [*process-id*]]

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced IPv6 ACL used to filter redistributed routes before advertisement, ranging from 2000 to 3999. Refer to "IPv6 ACL Configuration Commands" on page 2103 for ACL information.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to "IPv6 Routing Policy Configuration Commands" on page 1213 for IPv6 prefix list information.

route-policy-name: Name of a routing policy used to filter the redistributed routes before advertisement, a string of 1 to 19 characters. Refer to "Routing Policy

Common Configuration Commands" on page 1187 for routing policy information.

protocol: Filter routes redistributed from the specified routing protocol before advertisement. The routing protocol can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng** or **static** at present. If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.

process-id: Process ID of the routing protocol, ranging from 1 to 65535. This argument is available when the protocol is **isisv6**, **ospfv3** or **ripng**.

Description Use the **ipv6 filter-policy export** command to configure IPv6 IS-IS to filter redistributed routes before advertisement.

Use the **undo ipv6 filter-policy export** command to disable the filtering.

The filtering is disabled by default.

In some cases, only routes satisfying certain conditions will be advertised. You can configure the filtering conditions using the **ipv6 filter-policy** command.

You can use the **ipv6 filter-policy export** command, which filters redistributed routes only when they are advertised to other routers, in combination with the **ipv6 import-route** command.

- If no protocol is specified, routes redistributed from all protocols are filtered before advertisement.
- If a protocol is specified, only routes redistributed from the protocol are filtered before advertisement.

Related commands: **ipv6 filter-policy import**.

Examples # Reference the ACL6 2006 to filter all the redistributed routes before advertisement.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2006 export
```

ipv6 filter-policy import

Syntax **ipv6 filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } **import**

undo ipv6 filter-policy import

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced IPv6 ACL used to filter incoming routes, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter incoming routes, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter incoming routes, a string of 1 to 19 characters.

Description Use the **ipv6 filter-policy import** command to configure IPv6 IS-IS to filter the received routes.

Use the **undo ipv6 filter-policy import** command to disable the filtering.

The filtering is disabled by default.

In some cases, only the routing information satisfying certain conditions will be received. You can configure the filtering conditions using the **ipv6 filter-policy** command.

Related commands: **ipv6 filter-policy export**.

Examples # Reference the IPv6 ACL 2003 to filter the received routes.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 filter-policy 2003 import
```

ipv6 import-route

Syntax **ipv6 import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | [**level-1** | **level-2** | **level-1-2**] | **route-policy** *route-policy-name* | **tag** *tag*] *

undo ipv6 import-route *protocol* [*process-id*]

View IS-IS view

Parameters *protocol*: Redistributes routes from a specified routing protocol, which can be **direct**, **static**, **ripng**, **isisv6**, **bgp4+** or **ospfv3**.

process-id: Process ID of the routing protocol of **ripng**, **isisv6** or **ospfv3**, in the range of 1 to 65535. The default is 1.

cost: Cost for redistributed routes, ranging from 0 to 4261412864.

level-1: Redistributes routes into Level-1 routing table.

level-2: Redistributes routes into Level-2 routing table.

level-1-2: Redistributes routes into Level-1 and Level-2 routing tables.

route-policy-name: Name of a routing policy used to filter routes when they are being redistributed, a string of 1 to 19 characters.

tag: Specifies an administrative tag number for the redistributed routes, in the range of 1 to 4294967295.

allow-ibgp: Allows redistributing IBGP routes. This keyword is optional when the *protocol* is **bgp4+**.

Description Use the **ipv6 import-route** command to enable IPv6 IS-IS to redistribute routes from another routing protocol.

Use the **undo ipv6 import-route** command to disable route redistribution.

Route redistribution is disabled by default.

If no level is specified, the routes are imported to Level-2 routing table by default.

IPv6 IS-IS considers redistributed routes as routes to destinations outside the local routing domain.

You can specify a cost and a level for redistributed routes.

CAUTION: *Using the* ***import-route bgp4+ allow-ibgp*** *command will redistribute both EBGP and IBGP routes. The redistributed IBGP routes may cause routing loops. Therefore, be cautious with this command.*

Examples # Configure IPv6-IS-IS to redistribute static routes and sets the cost 15 for them.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1]ipv6 import-route static cost 15
```

ipv6 import-route isisv6 level-2 into level-1

Syntax **ipv6 import-route isisv6 level-2 into level-1** [**filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* | **route-policy** *route-policy-name* } | **tag** *tag*]*

undo ipv6 import-route isisv6 level-2 into level-1

View IS-IS view

Parameters *acl6-number*: Number of a basic or advanced ACL6 used to filter routes when they are leaking from Level-2 to Level-1, ranging from 2000 to 3999.

ipv6-prefix-name: Name of an IPv6 prefix list used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

route-policy-name: Name of a routing policy used to filter routes when they are leaking from Level-2 to Level-1, a string of 1 to 19 characters.

tag: Specifies an administrative tag number for the leaked routes, in the range of 1 to 4294967295.

Description Use the **ipv6 import-route isisv6 level-2 into level-1** to enable IPv6 IS-IS route leaking from Level-2 to Level-1.

Use the **undo ipv6 import-route isisv6 level-2 into level-1** command to disable the leaking.

The leaking is disabled by default.

The route leaking feature enables a Level-1-2 router to advertise routes destined to the Level-2 area and other Level-1 areas to the Level-1 and Level-1-2 routers in the local area.

Examples # Enable IPv6 IS-IS route leaking from Level-2 to Level-1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] ipv6 import-route isisv6 level-2 into level-1
```

ipv6 maximum load-balancing

Syntax **ipv6 maximum load-balancing** *number*

undo ipv6 maximum load-balancing

View IS-IS view

Parameters *number*: Maximum number of equivalent load-balanced routes.

Description Use the **ipv6 maximum load-balancing** command to configure the maximum number of equivalent load-balanced routes. Use the **undo ipv6 maximum load-balancing** command to restore the default.

Configure the maximum number of equivalent load-balanced routes according to the memory capacity.

Examples # Configure the maximum number of equivalent load-balanced routing as 2.

```
<Sysname> system-view
[Sysname] isis 100
[Sysname-isis-100] ipv6 maximum load-balancing 2
```

ipv6 preference

Syntax **ipv6 preference** { **route-policy** *route-policy-name* | *preference* } *

undo ipv6 preference

View IS-IS view

Parameters *preference*: Preference for IPv6 IS-IS, ranging from 1 to 255.

route-policy-name: Name of a routing policy, a string of 1 to 19 characters.

Description Use the **ipv6 preference** command to configure the preference for IPv6 IS-IS protocol.

Use the **undo ipv6 preference** command to configure the default preference for IPv6 IS-IS protocol.

The default preference is 15.

When a router runs multiple dynamic routing protocols at the same time, the system will assign a preference to each routing protocol. If several protocols find routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples # Configure the preference of IPv6 IS-IS protocol as 20.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 preference 20
```

ipv6 summary

Syntax **ipv6 summary** *ipv6-prefix prefix-length* [**avoid-feedback** | **generate_null0_route** | [**level-1** | **level-1-2** | **level-2**] | **tag** *tag*] *

undo ipv6 summary *ipv6-prefix prefix-length* [**level-1** | **level-1-2** | **level-2**]

View IS-IS view

Parameters *ipv6-prefix:* IPv6 prefix of the summary route.

prefix-length: Length of the IPv6 prefix, in the range of 0 to 128.

avoid-feedback: Specifies to avoid learning summary routes via routing calculation.

generate_null0_route: Generates the NULL 0 route to avoid routing loops.

level-1: Specifies to summarize only the routes redistributed to Level-1 area.

level-1-2: Specifies to summarize all the routes redistributed to Level-1 and Level-2 areas.

level-2: Specifies to summarize only the routes redistributed to Level-2 area.

tag: Value of an administrative tag, in the range of 1 to 4294967295.

*If no level is specified in the command, the default is **level-2**.*

Description Use the **ipv6 summary** command to configure an IPv6 IS-IS summary route.

Use the **undo ipv6 summary** command to remove the summary route.

Route summarization is disabled by default.

Configuring summary routes can reduce the size of the route table, LSPs and LSDB. Routes to be summarized can be IS-IS routes or redistributed routes. The cost of a summary route is the smallest cost among all summarized routes.

Examples # Configure a summary route of 2002::/32.

```
<Sysname> system-view
[Sysname] isis
[Sysname-isis-1] ipv6 summary 2002:: 32
```

isis ipv6 enable

Syntax **isis ipv6 enable** [*process-id*]

undo isis ipv6 enable

View Interface view

Parameters *process-id*: IS-IS process ID, ranging from 1 to 65535. The default is 1.

Description Use the **isis ipv6 enable** command to enable IPv6 for the specified IS-IS process on the interface.

Use the **undo isis ipv6 enable** command to disable the configuration.

IPv6 is disabled on the interface by default.

Examples # Enable global IPv6, create IS-IS routing process 1, enable IPv6 for the process, and enable IPv6 for the process on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] ipv6
[Sysname] isis 1
[Sysname-isis-1] network-entity 10.0001.1010.1020.1030.00
[Sysname-isis-1] ipv6 enable
[Sysname-isis-1] quit
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ipv6 address 2002::1/64
[Sysname-Serial2/0] isis ipv6 enable 1
```

84 IPv6 OSPFv3 Configuration Commands

abr-summary (OSPFv3 area view)

Syntax **abr-summary** *ipv6-address prefix-length* [**not-advertise**]

undo abr-summary *ipv6-address prefix-length*

View OSPFv3 area view

Parameters *ipv6-address*: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address, in the range 0 to 128. This argument specifies the number of consecutive 1s of the prefix, which defines the network ID.

not-advertise: Specifies not to advertise the summary IPv6 route.

Description Use the **abr-summary** command to configure an IPv6 summary route on an area border router.

Use the **undo abr-summary** command to remove an IPv6 summary route. Then the summarized routes are advertised.

By default, no route summarization is available on an ABR.

You can use this command only on an ABR to configure a summary route for the area. The ABR advertises only the summary route to other areas. Multiple contiguous networks may be available in an area, where you can summarize them with one route for advertisement.

Examples # Summarize networks 2000:1:1:1::/64 and 2000:1:1:2::/64 in Area 1 with 2000:1:1::/48.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] abr-summary 2000:1:1:: 48
```

area (OSPFv3 view)

Syntax **area** *area-id*

View OSPFv3 view

Parameters *area-id*: ID of an area, a decimal integer (in the range of 0 to 4294967295 and changed to IPv4 address format by the system) or an IPv4 address.

Description Use the **area** command to enter OSPFv3 area view.

The undo form of the command is not available. An area is removed automatically if there is no configuration and no interface is up in the area.

Examples # Enter OSPFv3 Area 0 view.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 0
[Sysname-ospfv3-1-area-0.0.0.0]
```

default cost

Syntax **default cost** *value*

undo default cost

View OSPFv3 view

Parameters *value*: Specifies a default cost for redistributed routes, in the range of 1 to 16777214.

Description Use the **default cost** command to configure a default cost for redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default cost is 1.

You need to configure the default cost value for redistributed routes to advertise them throughout the whole AS.

If multiple OSPFv3 processes are available, use of this command takes effect for the current process only.

Examples # Specify the default cost for redistributed routes as 10.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] default cost 10
```

default-cost (OSPFv3 area view)

Syntax **default-cost** *value*

undo default-cost

View OSPFv3 area view

Parameters *value*: Specifies a cost for the default route advertised to the stub area, in the range of 0 to 65535. The default is 1.

Description Use the **default-cost** command to specify the cost of the default route to be advertised to the stub area.

Use the **undo-default-cost** command to restore the default value.

Use of this command is only available on the ABR that is connected to a stub area.

You have two commands to configure a stub area: **stub**, **defaulted-cost**. You need to use the **stub** command on routers connected to a stub area to configure the area as stub.

If multiple OSPFv3 processes are running, use of this command takes effect only for the current process.

Related commands: **stub(OSPFv3 area view)**.

Examples # Configure Area1 as a stub area, and specify the cost of the default route advertised to the stub area as 60.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
[Sysname-ospfv3-1-area-0.0.0.1] default-cost 60
```

display debugging ospfv3

Syntax **display debugging ospfv3**

View Any view

Parameters None

Description Use the **display debugging ospfv3** command to display global OSPFv3 debugging state information.

Examples # Display the global OSPFv3 debugging state information.

```
<Sysname> display debugging ospfv3
OSPFv3 External route calculation debugging is on
```

display ospfv3

Syntax **display ospfv3** [*process-id*]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

Description Use the **display ospfv3** command to display OSPFv3 brief information. If no process ID is specified, OSPFv3 brief information about all processes will be displayed.

Examples # Display brief information about all OSPFv3 processes.

```
<Sysname> display ospfv3
Routing Process "OSPFv3 (1)" with ID 1.1.1.1
 SPF schedule delay 5 secs, Hold time between SPFs 10 secs
 Minimum LSA interval 5 secs, Minimum LSA arrival 1 secs
 Number of external LSA 0. These external LSAs' checksum Sum 0x0000
 Number of AS-Scoped Unknown LSA 0
 Number of LSA originated 3
 Number of LSA received 0
 Number of areas in this router is 1
  Area 0.0.0.1
       Number of interfaces in this area is 1
       SPF algorithm executed 1 times
       Number of LSA 2. These LSAs' checksum Sum 0x20C8
       Number of Unknown LSA 0
```

Table 298 Description on the fields of the display isofv3 command

Field	Description
Routing Process "OSPFv3 (1)" with ID 1.1.1.1	OSPFv3 process is 1, and router ID is 1.1.1.1.
SPF schedule delay	Delay interval of SPF calculation
Hold time between SPFs	Hold time between SPF calculations
Minimum LSA interval	Minimum interval for generating LSAs
Minimum LSA arrival	Minimum LSA repeat arrival interval
Number of external LSA	Number of ASEs
These external LSAs' checksum Sum	Sum of all the ASEs' checksum
Number of AS-Scoped Unknown LSA	Number of LSAs with unknown flooding scope
Number of LSA originated	Number of LSAs originated
Number of LSA received	Number of LSAs received
Number of areas in this router	Number of areas this router attached to
Area	Area ID
Number of interfaces in this area	Number of interfaces attached to this area
SPF algorithm executed 1 times	SPF algorithm is executed 1 time
Number of LSA	Number of LSAs

Table 298 Description on the fields of the display isofv3 command

Field	Description
These LSAs' checksum Sum	Sum of all LSAs' checksum
Number of Unknown LSA	Number of unknown LSAs

display ospfv3 interface

Syntax **display ospfv3 interface** [*interface-type interface-number* | **statistic**]

View Any view

Parameters *interface-type interface-number*: Interface type and interface number.

statistic: Displays the interface statistics.

Description Use the **display ospfv3 interface** command to display OSPFv3 interface information.

Examples # Display OSPFv3 interface information.

```
<Sysname> display ospfv3 interface serial 2/0
Serial2/0 is up, line protocol is up
  Interface ID 518
  IPv6 Prefixes
    FE80::1441:0:E213:1 (Link-Local Address)
    2000:1::1
  OSPFv3 Process (1), Area 0.0.0.1, Instance ID 0
    Router ID 2.2.2.2, Network Type POINTOPOINT, Cost: 1562
    Transmit Delay is 1 sec, State Point-To-Point, Priority 1
    No designated router on this link
     No backup designated router on this link
    Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
       Hello due in 00:00:02
   Neighbor Count is 1, Adjacent neighbor count is 1
```

Table 299 Description on the fields of the display ospfv3 interface command

Field	Description
Interface ID	Interface ID
IPv6 Prefixes	IPv6 Prefix
OSPFv3 Process	OSPFv3 Process
Area	Area ID
Instance ID	Instance ID
Router ID	Router ID
Network Type	Network type of the interface
Cost	Cost value of the interface
Transmit Delay	Transmission delay of the interface
State	Interface state
Priority	DR priority of the interface
No designated router on this link	No designated router on this link
No backup designated router on this link	No backup designated router on this link

Table 299 Description on the fields of the display ospfv3 interface command

Field	Description
Timer interval configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Time intervals in seconds configured on the interface, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Hello packet will be sent in 2 seconds
Neighbor Count	Number of Neighbors on the interface
Adjacent neighbor count	Number of Adjacencies on the interface

display ospfv3 lsdb

Syntax **display ospfv3** [*process-id*] **lsdb** [[**external** | **inter-prefix** | **inter-router** | **intra-prefix** | **link** | **network** | **router**] [*link-state-id*] [**originate-router** *router-id*] | **total**]

View Any view

Parameters *process-id*: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

external: Specifies to display information about AS-external LSAs.

inter-prefix: Specifies to display information about Inter-area-prefix LSAs.

inter-router: Specifies to display information about Inter-area-router LSAs.

intra-prefix: Specifies to display information about Intra-area-prefix LSAs.

link: Specifies to display information about Link-LSAs.

network: Specifies to display information about Network-LSAs.

router: Specifies to display information about Router-LSAs.

link-state-id: Link state ID, an IPv4 address.

originate-router *router-id*: The ID of the advertising router.

total: Specifies to display all information in the LSDB.

Description Use the **display ospfv3 lsdb** command to display OSPFv3 LSDB information.

Examples # Display OSPFv3 LSDB information.

```
<Sysname> display ospfv3 lsdb

            OSPFv3 Router with ID (5.5.5.5) (Process 1)
               Link-LSA (Interface Ethernet1/0)
 ----------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum  Prefix
0.15.0.9        5.5.5.5          0304  0x80000001 0x5b6a      1
0.15.0.9        6.6.6.6          0311  0x80000001 0x6956      1

               Router-LSA (Area 0.0.0.0)
```

```
 ------------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum    Link
0.0.0.0         5.5.5.5          0263  0x80000002 0x823f      1
0.0.0.0         6.6.6.6          0264  0x80000003 0x625a      1

               Network-LSA (Area 0.0.0.0)
 ------------------------------------------------------------------
Link State ID   Origin Router    Age   SeqNum     CkSum
0.15.0.9        6.6.6.6          0264  0x80000001 0x3498

               Intra-Area-Prefix-LSA (Area 0.0.0.0)
 ------------------------------------------------------------------
Link State ID  Origin Router   Age   SeqNum     CkSum  Prefix  Reference
0.0.0.2        6.6.6.6         0263  0x80000001 0x95c4      1  Network-LSA
```

Table 300 Description on the fields of the display isofv3 lsdb command

Field	Description
Link-LSA	Type 8 LSA
Link State ID	Link State ID
Origin Router	Originating Router
Age	Age of LSAs
SeqNum	LSA sequence number
CkSum	LSA Checksum
Prefix	Number of Prefixes
Router-LSA	Router-LSA
Link	Number of links
Network-LSA	Network-LSA
Intra-Area-Prefix-LSA	Type 9 LSA
Reference	Type of referenced LSA

Display Link-local LSA information in the LSDB.

```
<Sysname> display ospfv3 lsdb link
            OSPFv3 Router with ID (2.2.2.2) (Process 1)

                Link-LSA (Interface Serial2/0)

  LS age: 11
  LS Type: Link-LSA
  Link State ID: 0.0.2.6
  Originating Router: 2.2.2.2
  LS Seq Number: 0x80000002
  Checksum: 0xEFFA
  Length: 56
  Priority: 1
  Options: 0x000013 (-|R|-|-|E|V6)
  Link-Local Address: FE80::1441:0:E213:1
  Number of Prefixes: 1
    Prefix: 2000:1::/64
    Prefix Options: 0 (-|-|-|-)
```

Table 301 Description on the fields of the display ospfv3 lsdb command

Field	Description
LS age	Age of LSA
LS Type	Type of LSA

Table 301 Description on the fields of the display ospfv3 lsdb command

Field	Description
Originating Router	Originating Router
LS Seq Number	LSA Sequence Number
Checksum	LSA Checksum
Length	LSA Length
Priority	Router Priority
Options	Options
Link-Local Address	Link-Local Address
Number of Prefixes	Number of Prefixes
Prefix	Address prefix
Prefix Options	Prefix options

display ospfv3 lsdb statistic

Syntax **display ospfv3 lsdb statistic**

View Any view

Parameters None

Description Use the **display ospfv3 lsdb statistic** command to display LSA statistics in the OSPFv3 LSDB.

Examples # Display OSPFv3 LSDB statistics.

```
<System> display ospfv3 lsdb statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                        LSA Statistics
 ----------------------------------------------------------------------
Area ID         Router   Network  InterPre InterRou IntraPre Link     ASE
0.0.0.0         2        1        1        0        1
0.0.0.1         1        0        1        0        1
Total           3        1        2        0        2        3        0
```

Table 302 Descriptions on the fields of the display ospfv3 lsdb statistic command

Field	Description
Area ID	Area ID
Router	Router-LSA number
Network	Network-LSA number
InterPre	Inter-Area-Prefix-LSA number
InterRou	Inter-Area-Router-LSA number
IntraPre	Intra-Area-Prefix-LSA number
Link	Link-LSA number
ASE	AS-external-LSA number
Total	Total LSA number

display ospfv3 next-hop

Syntax **display ospfv3** [*process-id*] **next-hop**

View Any view

Parameters *process-id*: Specifies ID of an OSPFv3 process, ranging from 1 to 65535.

Description Use the **display ospfv3 next-hop** command to display OSPFv3 next hop information.

If no process is specified, next hop information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 next hop information.

```
<Sysname> display ospfv3 next-hop

            OSPFv3 Router with ID (2.2.2.2) (Process 1)
Neighbor-Id     Next-Hop                              Interface   RefCount
1.1.1.1         FE80::20F:E2FF:FE00:1                 Eth1/0      1
```

Table 303 Description on the fields of the display ospfv3 next-hop command

Field	Description
Neighbor-Id	Neighboring router ID
Next-hop	Next-hop address
Interface	Outbound interface
RefCount	Reference count

display ospfv3 peer

Syntax **display ospfv3** [*process-id*] [**area** *area-id*] **peer** [[*interface-type interface-number*] [**verbose**] | *peer-router-id*]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

area: Specifies to display neighbor information of the specified area.

area-id: The ID of an area, a decimal integer that is translated into IPv4 address format by the system (in the range of 0 to 4294967295) or an IPv4 address.

interface-type interface-number: interface type and number.

verbose: Display detailed neighbor information.

peer-router-id: Router-ID of the specified neighbor.

Description Use the **display ospfv3 peer** command to display OSPFv3 neighbor information.

- If no *area-id* is specified, the neighbor information of all areas is displayed.
- If no *process-id* is specified, the information of all processes is displayed.
- If no interface or neighbor Router-ID is specified, the neighbor information of all interfaces is displayed.

Examples # Display the neighbor information of OSPFv3 process 1 on an interface.

```
<Sysname> display ospfv3 1 peer serial 2/0
                    OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1)
Neighbor ID     Pri   State            Dead Time   Interface  Instance ID
1.1.1.1         1     Full/ -          00:00:33    S2/0       0
```

Table 304 Description on the fields of the display isofv3 peer command

Field	Description
Neighbor ID	Neighbor ID
Pri	Priority of neighbor router
State	Neighbor state
Dead Time	Dead time remained
Interface	Interface connected to the neighbor
Instance ID	Instance ID

Display detailed neighbor information of OSPFv3 process 100 of an interface.

```
<Sysname> display ospfv3 100 peer serial 2/0 verbose
OSPFv3 Process (100)
 Neighbor: 1.1.1.1, interface address: FE80::3D43:0:8C14:1
    In the area 0.0.0.1 via interface Serial2/0
    DR is 0.0.0.0 BDR is 0.0.0.0
    Options is 0x000013 (-|R|-|-|E|V6)
    Dead timer due in 00:00:29
    Neighbor is up for 00:06:28
    Database Summary List 0
    Link State Request List 0
    Link State Retransmission List 0
```

Table 305 Description on the fields of the display isofv3 peer verbose command

Field	Description
Neighbor	Neighbor ID
interface address	Interface address
In the area 0.0.0.1 via interface Serial2/0	Interface Serial 2/0 belongs to area 1
DR is 0.0.0.0 BDR is 0.0.0.0	No DR or BDR is selected
Options is 0x000013 (-|R|-|-|E|V6)	The option is 0x000013 (-|R|-|-|E|V6)
Dead timer due in 00:00:29	Dead timer due in 00:00:29
Neighbor is up for 00:06:28	Neighbor is up for 00:06:28
Database Summary List	Number of LSAs sent in DD packet
Link State Request List	Number of LSAs in the link state request list
Link State Retransmission List	Number of LSAs in the link state retransmission list

display ospfv3 peer statistic

Syntax **display ospfv3 peer statistic**

View Any view

Parameters None

Description Use the **display ospfv3 peer statistic** command to display information about all OSPFv3 neighbors on the router, that is, numbers of neighbors in different states.

Examples # Display information about all OSPFv3 neighbors.

```
<Sysname> display ospfv3 peer statistic

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          Neighbor Statistics
 ------------------------------------------------------------------------
Area ID          Down     Init     2-way    ExStar   Exchange Loading  Full
0.0.0.0          0        0        0        0        0        0        1
Total            0        0        0        0        0        0        1
```

Table 306 Description on the fields of the display ospfv3 peer statistic command

Field	Description
Area ID	Area ID
Down	In this state, neighbor initial state, the router has not received any information from a neighboring router for a period of time.
Init	In this state, the router received a Hello packet from the neighbor but the packet gives no ID of the router. Mutual communication is not available.
2-Way	Indicates mutual communication between the router and its neighbor is available. DR/BDR election is finished under this state (or higher).
ExStart	In this state, the router decides on the initial DD sequence number and master/slave relationship of the two parties.
Exchange	In this state, the router exchanges DD packets with the neighbor.
Loading	In this state, the router send LSRs to request the neighbor for needed LSAs.
Full	Indicates LSDB synchronization has been accomplished between neighbors.
Total	Total number of neighbors under the same state

display ospfv3 request-list

Syntax **display ospfv3** [*process-id*] **request-list** [**statistics**]

View Any view

Parameters *process-id*: OSPFv3 process ID, in the range 1 to 65535.

statistics: Statistics of link state request list.

Description Use the **display ospfv3 request-list** command to display OSPFv3 link state request list.

If no process is specified, link state request list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
             Interface  Eth1/0    Area-ID   0.0.0.1
 ------------------------------------------------------------------------
                         Nbr-ID   2.2.2.2
LS-Type              LS-ID           AdvRouter       SeqNum       Age
AS-External-LSA      0.0.16.66       2.2.2.2         0x80000001   98
AS-External-LSA      0.0.16.67       2.2.2.2         0x80000001   98
AS-External-LSA      0.0.16.68       2.2.2.2         0x80000001   98
```

Table 307 Description on the fields of the display ospfv3 request-list command

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising router
SeqNum	LSA sequence number
Age	Age of LSA

Display the statistics of OSPFv3 link state request list.

```
<Sysname> display ospfv3 request-list statistics

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
Interface   Neighbor        LSA-Count
Eth1/0          2.2.2.2          0
```

Table 308 Description on the fields of the display ospfv3 request-list statistics command

Field	Description
Interface	Interface name
Neighbor	Neighbor router ID
LSA-Count	Number of LSAs in the request list

display ospfv3 retrans-list

Syntax **display ospfv3** [*process-id*] **retrans-list** [**statistics**]

View Any view

Parameters *process-id*: OSPFv3 process ID, in the range 1 to 65535.

statistics: Displays link state retransmission list statistics.

Description Use the **display ospfv3 retrans-list** command to display OSPFv3 link state retransmission list.

If no process is specified, link state retransmission list information of all OSPFv3 processes is displayed.

Examples # Display the information of OSPFv3 link state retransmission list.

```
<Sysname> display ospfv3 retrans-list
            OSPFv3 Router with ID (2.2.2.2) (Process 1)
             Interface  Eth1/0    Area-ID   0.0.0.1
 ----------------------------------------------------------------------
                          Nbr-ID   2.2.2.2
LS-Type                LS-ID           AdvRouter       SeqNum       Age
Router-LSA             0.0.0.0         2.2.2.2         0x80000006   0
Network-LSA            0.15.0.8        2.2.2.2         0x80000001   0
Intra-Area-Prefix-LSA  0.0.0.1         2.2.2.2         0x80000006   0
```

Table 309 Description on the fields of the display ospfv3 retrans-list command

Field	Description
Interface	Interface name
Area-ID	Area ID
Nbr-ID	Neighbor router ID
LS-Type	Type of LSA
LS-ID	Link state ID
AdvRouter	Advertising Router
SeqNum	LSA sequence Number
Age	Age of LSA

Display the statistics of OSPFv3 link state retransmission list.

```
<Sysname>display ospfv3 retrans-list statistics

            OSPFv3 Router with ID (3.3.3.3) (Process 1)
Interface  Neighbor        LSA-Count
Eth1/0     1.1.1.1           0
```

Table 310 Description on the fields of the display ospfv3 retrans-list statistics command

Field	Description
Interface	Interface name
Neighbor	Neighbor ID
LSA-Count	Number of LSAs in the retransmission request list

display ospfv3 routing

Syntax **display ospfv3** [*process-id*] **routing** [*ipv6-address prefix-length* | *ipv6-prefix /prefix-length* | **abr-routes** | **asbr-routes** | **all** | **statistics**]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

ipv6-address: IPv6 address prefix.

prefix-length: Prefix length, in the range 0 to 128.

abr-routes: Specifies to display routes to ABR.

asbr-routes: Specifies to display routes to ASBR.

all: Specifies to display all routes.

statistics: Specifies to display the statistics of OSPFv3 routing table.

Description Use the **display ospfv3 routing** command to display OSPFv3 routing table information.

If no process is specified, routing table information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 routing table information.

```
<Sysname> display ospfv3 routing

 E1 - Type 1 external route,    IA - Inter area route,    I  - Intra area route
 E2 - Type 2 external route,    *  - Selected route

            OSPFv3 Router with ID (1.1.1.1) (Process 1)
 ------------------------------------------------------------------------
 *Destination: 2001::/64
  Type       : I                                      Cost     : 1
  NextHop    : directly-connected                     Interface: Eth1/0
```

Table 311 Description on the fields of the display ospfv3 routing command

Field	Description
Destination	Destination network segment
Type	Route type
Cost	Route cost value
Next-hop	Next hop address
Interface	Outbound interface

Display the statistics of OSPFv3 routing table.

```
<Sysname> display ospfv3 routing statistics
            OSPFv3 Router with ID (1.1.1.1) (Process 1)
                          OSPFv3 Routing Statistics
 Intra-area-routes   :   1
 Inter-area-routes   :   0
 External-routes     :   0
```

Table 312 Description on the fields of the display ospfv3 routing statistics command

Field	Description
Intra-area-routes	Number of Intra-area-routes
Inter-area-routes	Number of inter-area routes
External-routes	Number of external routes

display ospfv3 statistic

Syntax **display ospfv3 statistic**

View Any view

Parameters None

Description Use the **display ospfv3 statistic** command to display outbound/inbound OSPFv3 packet statistics on associated interface(s).

Examples # Display outbound/inbound OSPFv3 packet statistics on associated interfaces.

```
<Sysname> display ospfv3 statistic

                        OSPFv3 Statistics
Interface Ethernet1/0 Instance 0
 Type               Input       Output
 Hello              189         63
 DB Description     10          8
 Ls Req             2           1
 Ls Upd             16          6
 Ls Ack             10          6
```

Table 313 Description on the fields of the display ospfv3 statistics command

Field	Description
Interface	Interface name
Instance	Instance number
Type	Type of packet
Input	Number of packets received by the interface
Output	Number of packets sent by the interface
Hello	Hello packet
DB Description	Database description packet
Ls Req	Link state request packet
Ls Upd	Link state update packet
Ls Ack	Link state acknowledgement packet

display ospfv3 topology

Syntax **display ospfv3** [*process-id*] **topology** [**area** *area-id*]

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process of which to display topology information, ranging from 1 to 65535.

area: Display the topology information of the specified area.

area-id: The ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

Description Use the **display ospfv3 topology** command to display OSPFv3 topology information. If no process is specified, topology information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 area 1 topology information.

```
<Sysname> display ospfv3 topology area 1

                      OSPFv3 Process (1)
OSPFv3 Area (0.0.0.1) topology
Type  ID(If-Index)       Bits      Metric    Next-Hop        Interface
Rtr   1.1.1.1                      --
Rtr   2.2.2.2                      1         2.2.2.2         Eth1/0
Rtr   3.3.3.3                      1         3.3.3.3         Eth1/0
Rtr   4.4.4.4                      1         4.4.4.4         Eth1/0
Net   4.4.4.4(983049)              1         0.0.0.0         Eth1/0
```

Table 314 Description on the fields of the display ospfv3 topology command

Field	Description
Type	Type of node
ID(If-Index)	Router ID
Bits	Flag bit
Metric	Cost value
Next-Hop	Next hop
Interface	Outbound interface

display ospfv3 vlink

Syntax **display ospfv3** [*process-id*] **vlink**

View Any view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

Description Use the **display ospfv3 vlink** command to display OSPFv3 virtual link information. If no process is specified, virtual link information of all OSPFv3 processes is displayed.

Examples # Display OSPFv3 virtual link information.

```
<Sysname> display ospfv3 vlink
     Virtual Link VLINK1 to router 1.1.1.1 is up
       Transit area :0.0.0.1 via interface Serial2/0, instance ID: 0
       Local address: 2000:1::1
       Remote address: 2001:1:1::1
       Transmit Delay is 1 sec, State: P-To-P,
       Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Re
transmit: 5
```

```
Hello due in 00:00:02
Adjacency state :Full
```

Table 315 Description on the fields of the display ospfv3 vlink command

Field	Description
Virtual Link VLINK1 to router 1.1.1.1 is up	The virtual link VLINK1 to router 1.1.1.1 is up
Transit area 0.0.0.1 via interface Serial2/0	Interface Serial 2/0 in transit area 0.0.0.1.
instance ID	Instance ID
Local address	Local IPv6 address
Remote address	Remote IPv6 address
Transmit Delay	Transmit delay of sending LSAs
State	Interface state
Timer intervals configured, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5	Timer intervals in seconds, Hello: 10, Dead: 40, Wait: 40, Retransmit: 5
Hello due in 00:00:02	Send hello packets in 2 seconds.
Adjacency state	Adjacency state

filter-policy export(OSPFv3 view)

Syntax **filter-policy** { *acl-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

undo filter-policy export [**isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static**]

View OSPFv3 view

Parameters *acl-number*: Specifies the ACL number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

isisv6 *process-id*: Specifies to filter the routes of an IPv6 IS-IS process, which is in the range of 1 to 65535.

ospfv3 *process-id*: Specifies to filter the routes of an OSPFv3 process, which is in the range of 1 to 65535.

ripng *process-id*: Specifies to filter the routes of a RIPng process, which in the range of 1 to 65535.

bgp4+: Specifies to filter BGP4+ routes.

direct: Specifies to filter direct routes.

static: Specifies to filter static routes.

Description Use the **filter-policy export** command to filter redistributed routes.

Use the **undo filter-policy export** command to remove the configuration.

If no protocol is specified, all redistributed routes will be filtered.

By default, IPv6 OSPFv3 does not filter redistributed routes.

*Using the **filter-policy export** command filters only routes redistributed by the **import-route** command. If the **import-route** command is not configured to redistribute routes from other protocols and other OSPFv3 processes, use of the **filter-policy export** command does not take effect.*

Examples # Filter all redistributed routes using IPv6 ACL 2001.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2000] rule permit source 2002:1:: 64
[Sysname-acl6-basic-2000] quit
[Sysname] ospfv3
[Sysname-ospfv3-1] filter-policy 2001 export
```

filter-policy import(OSPFv3 view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View OSPFv3 view

Parameters *acl6-number*: Specifies an ACL number, ranging from 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list, a string of up to 19 characters.

Description Use the **filter-policy import** command to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

No received routes are filtered by default.

*Using the **filter-policy import** command only filters routes computed by OSPFv3. The routes that fail to pass are not added to the routing table.*

Examples # Filter received routes using the IPv6 prefix list **abc**.

```
<Sysname> system-view
[Sysname] ip ipv6-prefix abc permit 2002:1:: 64
[Sysname] ospfv3 1
[Sysname-ospfv3-1] filter-policy ipv6-prefix abc import
```

import-route(OSPFv3 view)

Syntax **import-route** { **isisv6** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** [**allow-ibgp**] | **direct** | **static** } [**cost** *value* | **type** *type* | **route-policy** *route-policy-name*]*

undo import-route { **isis** *process-id* | **ospfv3** *process-id* | **ripng** *process-id* | **bgp4+** | **direct** | **static** }

View OSPFv3 view

Parameters **isisv6** *process-id*: Specifies a process ID of ISIS to redistribute ISIS routes with the process ID, in the range 1 to 65535.

ospfv3 *process-id*: Specifies a process ID of OSPFv3 to redistribute OSPFv3 routes with the process ID, in the range 1 to 65535.

ripng *process-id*: Specifies a process ID of **ripng** to redistribute **ripng** routes with the process ID, in the range 1 to 65535.

bgp4+: Specifies to redistribute **bgp4+** routes.

allow-ibgp: Allows redistributing IBGP route.

direct: Specifies to redistribute **direct** routes.

static: Specifies to redistributes **static** routes.

cost *value*: Specifies the cost for redistributed routes, ranging from 1 to 16777214. It defaults to 1.

type *type*: Specifies the type for redistributed routes, 1 or 2. It defaults to 2.

route-policy *route-policy-name*: Specifies to redistribute only the routes that match the specified route-policy. *route-policy-name* is a string of up to 19 characters.

CAUTION: *Using the* ***import-route bgp4+*** *command redistributes only EBGP routes, while using the* ***import-route bgp4+ allow-ibgp*** *command redistributes both EBGP and IBGP routes.*

Description Use the **import-route** command to redistribute routes.

Use the **undo import-route** command to disable routes redistribution.

IPv6 OSPFv3 does not redistribute routes from other protocols by default.

Examples # Configure to redistribute routes from RIPng and specify the type as type 2 and cost as 50.

```
<Sysname> system-view
[Sysname] ospfv3
[Sysname-ospfv3-1] import-route ripng 10 type 2 cost 50
```

Configure OSPFv3 process 100 to redistribute the routes found by OSPFv3 process 160.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] import-route ospfv3 160
```

log-peer-change

Syntax **log-peer-change**

undo log-peer-change

View OSPFv3 view

Parameters None

Description Use the **log-peer-change** command to enable the logging on neighbor state changes.

Use the **undo maximum load-balancing** command to disable the logging.

With this feature enabled, information about neighbor state changes of the current OSPFv3 process will display on the configuration terminal.

Examples # Disable the logging on neighbor state changes of OSPFv3 process 100.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] undo log-peer-change
```

maximum load-balancing(OSPFv3 view)

Syntax **maximum load-balancing** *maximum*

undo maximum load-balancing

View OSPFv3 view

Parameters *maximum*: Maximum number of load-balanced routes, in the range 1 to 8. The argument being set to 1 means no load balancing is available.

Description Use the **maximum load-balancing** command to configure the maximum number of load-balanced routes.

Use the **undo maximum load-balancing** command to restore the default.

Examples # Configure the maximum load-balanced routes as 6.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] maximum load-balancing 6
```

ospfv3

Syntax **ospfv3** [*process-id*]

undo ospfv3 [*process-id*]

View System view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535. The process ID defaults to 1.

Description Use the **ospfv3** command to enable an OSPFv3 process and enter OSPFv3 view.

Use the **undo ospfv3** command to disable an OSPFv3 process.

The system runs no OSPFv3 process by default.

Related commands: **router-id**.

An OSPFv3 process can run normally only when Router ID is configured in OSPFv3 view. Otherwise, you can find the process, but which cannot generate any LSA.

Examples # Enable the OSPFv3 process with process ID as 120 and configure the Router ID as 1.1.1.1.

```
<Sysname> system-view
[Sysname] ospfv3 120
[Sysname-ospfv3-120] router-id 1.1.1.1
```

ospfv3 area

Syntax **ospfv3** *process-id* **area** *area-id* [**instance** *instance-id*]

undo ospfv3 *process-id* **area** *area-id* [**instance** *instance-id*]

View Interface view

Parameters *process-id*: Specifies the ID of an OSPFv3 process, ranging from 1 to 65535.

area-id: The ID of an area, a decimal integer (in the range of 0 to 4294967295) that is translated into IPv4 address format by the system or an IPv4 address.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 area** command to enable an OSPFv3 process on the interface and specify the area for the process.

Use the **undo ospfv3 area** command to disable an OSPFv3 process.

OSPFv3 is not enabled on an interface by default.

Examples # Enable OSPFv3 process 1 on an interface that belongs to instance 1 and specify area 1 for the process.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-serial2/0] ospfv3 1 area 1 instance 1
```

ospfv3 cost

Syntax **ospfv3 cost** *value* [**instance** *instance-id*]

undo ospfv3 cost [**instance** *instance-id*]

View Interface view

Parameters *value*: OSPFv3 cost of the interface, in the range 1 to 65535.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 cost** command to configure the OSPFv3 cost on an interface of an instance.

Use the **undo ospfv3 cost** command to restore the default OSPFv3 cost on an interface of an instance.

By default, a router's interface automatically calculates the OSPFv3 cost based on its bandwidth.

Examples # Specifies the OSPFv3 cost as 33 on an interface of instance 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospfv3 cost 33 instance 1
```

ospfv3 dr-priority

Syntax **ospfv3 dr-priority** *priority* [**instance** *instance-id*]

undo ospfv3 dr-priority [**instance** *instance-id*]

View Interface view

Parameters *priority*: DR priority, in the range 0 to 255.

instance-id: ID of the instance an interface belongs to, in the range 0 to 255, which defaults to 0.

Description Use the **ospfv3 dr-priority** command to set the DR priority for an interface of an instance.

Use the **undo ospfv3 dr-priority** command to restore the default value.

The DR priority on an interface defaults to 1

An interface's DR priority determines its privilege for DR/BDR selection, and the interface with the highest priority is considered first.

Examples # Set the DR priority for an interface of instance 1 to 8.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospfv3 dr-priority 8 instance 1
```

ospfv3 mtu-ignore

Syntax **ospfv3 mtu-ignore** [**instance** *instance-id*]

undo ospfv3 mtu-ignore [**instance** *instance-id*]

View Interface view

Parameters *instance-id*: Instance ID, in the range 0 to 255, which defaults to 0.

Description Use the **ospfv3 mtu-ignore** command to configure an interface to ignore MTU when sending DD packets.

Use the **undo ospfv3 mtu-ignore** command to restore the default configuration.

MTU is not ignored by default.

Examples # Configure an interface that belongs to instance 1 to ignore MTU.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospfv3 mtu-ignore instance 1
```

ospfv3 timer dead

Syntax **ospfv3 timer dead** *seconds* [**instance** *instance-id*]

undo ospfv3 timer dead [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Dead time in seconds, ranging from 1 to 65535,

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer dead** command to configure the OSPFv3 neighbor dead time for an interface that belongs to a specified instance.

Use the **undo ospfv3 timer dead** command to restore the default.

By default, the OSPFv3 neighbor dead time is 40 seconds for P2P and Broadcast interfaces, and is not supported on P2MP and NBMA interfaces at present.

OSPFv3 neighbor dead time: if an interface receives no hello packet from a neighbor after dead time elapses, the interface will considers the neighbor is dead.

The **dead** *seconds* value is at least four times the **Hello** *seconds* value and must be identical on interfaces attached to the same network segment.

Related commands: **ospfv3 timer hello**.

Examples # Configure the OSPFv3 neighbor dead time as 80 seconds for an interface with instance 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospfv3 timer dead 80 instance 1
```

ospfv3 timer hello

Syntax **ospfv3 timer hello** *seconds* [**instance** *instance-id*]

undo ospfv3 timer hello [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Interval between hello packets, ranging from 1 to 65535.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer hello** command to configure the hello interval for an interface that belongs to an instance.

Use the **undo ospfv3 timer hello** command to restore the default.

By default, the hello interval is 10 seconds for P2P and Broadcast interfaces, and is not supported on the P2MP or NBMA interfaces at present.

Related commands: **ospfv3 timer dead**.

Examples # Configure the hello interval as 20 seconds for an interface of instance 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] ospfv3 timer hello 20 instance 1
```

ospfv3 timer retransmit

Syntax **ospfv3 timer retransmit** *interval* [**instance** *instance-id*]

undo ospfv3 timer retransmit [**instance** *instance-id*]

View Interface view

Parameters *interval*: Specifies LSA retransmission interval in seconds for an interface, ranging from 1 to 65535.

instance-id: The instance ID of an interface, in the range of 0 to 255, which defaults to 0.

Description Use the **ospfv3 timer retransmit** command to configure the LSA retransmission interval for an interface of an instance.

Use the **undo ospfv3 timer retransmit** command to restore the default.

The interval defaults to 5 seconds.

When a router sends a LSA to its neighbor, it waits for an acknowledgement. If receiving no acknowledgement after retransmission interval elapses, it will retransmit the LSA.

The LSA retransmission interval should not be too small for avoidance of unnecessary retransmissions.

Examples # Configure the LSA retransmission interval on an interface of instance 1 as 12 seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospfv3 timer retransmit 12 instance 1
```

ospfv3 trans-delay

Syntax **ospfv3 trans-delay** *seconds* [**instance** *instance-id*]

undo ospfv3 trans-delay [**instance** *instance-id*]

View Interface view

Parameters *seconds*: Transmission delay in seconds, ranging from 1 to 3600. The default is 1.

instance-id: The instance ID of an interface, in the range of 0 to 255, with the default as 0.

Description Use the **ospfv3 trans-delay** command to configure the transmission delay for an interface with an instance ID.

Use the **undo ospfv3 trans-delay** command to restore the default.

The transmission delay defaults to 1s.

As LSAs are aged in the LSDB (incremented 1 by each second) but not aged on transmission, it is necessary to add a delay time to the age time before sending a LSA. This configuration is important for low-speed networks.

Examples # Configure the transmission delay as 3 seconds for an interface of instance 1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ospfv3 trans-delay 3 instance 1
```

preference

Syntax **preference** [**ase**] [**route-policy** *route-policy-name*] *preference*

undo preference [**ase**]

View OSPFv3 view

Parameters **ase**: Applies the preference to OSPFv3 external routes. If the keyword is not specified, the preference applies to OSPFv3 internal routes.

route-policy *route-policy-name*: References a routing policy to set preference for specific routes. The name is a string of 1 to 19 characters.

preference: Preference of OSPFv3, in the range 1 to 255.

Description Use the **preference** command to specify a preference for OSPFv3 routes.

Use the **undo preference** command to restore the default.

By default, the preference for OSPFv3 internal routes is 10, and that for OSPFv3 external routes is 150.

The smaller the value is, the higher the preference is.

A router may run multiple routing protocols. Each protocol has a preference. When several routing protocols find multiple routes to the same destination, the route found by the protocol with the highest preference is selected.

Examples # Set a preference of 150 for OSPFv3 routes.

```
<Sysname> system-view
[Sysname] OSPFv3
[Sysname-OSPFv3-1] preference 150
```

router-id

Syntax **router-id** *router-id*

undo router-id

View OSPFv3 view

Parameters *router-id*: A 32-bit router ID, in IPv4 address format.

Description Use the **router-id** command to configure the OSPFv3 router ID.

Use the **undo router-id** command to remove a configured router ID.

Router ID is the unique identification of an OSPF process in an autonomous system. An OSPFv3 process cannot run without a Router ID.

Make sure that different processes have different Router IDs.

Related commands: **ospfv3**.

By configuring different router IDs for different processes, you can run multiple OSPFv3 processes on a router.

Examples # Configure the Router ID as 10.1.1.3 for OSPFv3 process 1.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] router-id 10.1.1.3
```

silent-interface(OSPFv3 view)

Syntax **silent-interface** { *interface-type interface-number* | **all** }

undo silent-interface { *interface-type interface-number* | **all** }

View OSPFv3 view

Parameters *interface-type interface-number*: Interface type and number

all: Specifies all interfaces.

Description Use the **silent-interface** command to disable the specified interface from sending OSPFv3 packets.

Use the **undo silent-interface** command to restore the default.

An interface is able to send OSPFv3 packets by default.

Multiple processes can disable the same interface from sending OSPFv3 packets, but use of the **silent-interface** command takes effect only on interfaces enabled with the current process.

Examples # Disable an interface from sending OSPFv3 packets in OSPFv3 processes 100 and 200.

```
<Sysname> system-view
[Sysname] ospfv3 100
[Sysname-ospfv3-100] router-id 10.110.1.9
[Sysname-ospfv3-100] silent-interface ethernet 1/0
[Sysname-ospfv3-100] quit
[Sysname] ospfv3 200
[Sysname-ospfv3-200] router-id 20.18.0.7
[Sysname-ospfv3-200] silent-interface ethernet 1/0
```

spf timers

Syntax **spf timers** *delay-interval hold-interval*

undo spf timers

View OSPFv3 view

Parameters *delay-interval*: The interval in seconds between when OSPFv3 receives a topology change and when it starts SPF calculation. in the range 1 to 65535.

hold-interval: The hold interval in seconds between two SPF calculations, in the range 1 to 65535.

Description Use the **spf timers** command to configure the delay interval and hold interval for OSPFv3 SPF calculation.

Use the **undo spf timers** command to restore the default.

The delay interval and hold interval default to 5s and 10s.

An OSPFv3 router works out a shortest path tree with itself as root based on the LSDB, and decides on the next hop to a destination network according the tree. Adjusting the SPF calculation interval can restrain bandwidth and router resource from over consumption due to frequent network changes.

Examples # Configure the delay interval and hold interval as 6 seconds for SPF calculation.

```
<Sysname> system-view
[Sysname]ospfv3 1
[Sysname-ospfv3-1] spf timers 6 6
```

stub(OSPFv3 area view)

Syntax **stub** [**no-summary**]

undo stub

View OSPFv3 area view

Parameters **no-summary**: This argument is only applicable to the ABR of a stub area. With it configured, the ABR advertises only a default route in a Summary-LSA to the stub area (such an area is called a totally stub area).

Description Use the **stub** command to configure an area as a stub area.

Use the **undo stub** command to remove the configuration.

By default, an area is not configured as a stub area.

When an area is configured as a stub area, all the routers attached to the area must be configured with the **stub** command.

Related commands: **default cost**.

Examples # Configure OSPFv3 area 1 as a stub area.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 1
[Sysname-ospfv3-1-area-0.0.0.1] stub
```

vlink-peer(OSPFv3 area view)

Syntax **vlink-peer** *router-id* [**hello** *seconds* | **retransmit** *seconds* | **trans-delay** *seconds* | **dead** *seconds* | **instance** *instance-id*] *

undo vlink-peer *router-id* [**hello** | **retransmit** | **trans-delay** | **dead**]*

View OSPFv3 area view

Parameters *router-id*: Router ID for a virtual link neighbor.

hello *seconds*: Specifies the interval in seconds of sending Hello packets, ranging from 1 to 8192, with the default as 10. This value must equal to the **hello** *seconds* configured on the virtual link peer router.

retransmit *seconds*: Specifies the interval in seconds of retransmitting LSA packets, ranging from 1 to 3600, with the default as 5.

trans-delay *seconds*: Specifies the delay interval in seconds of sending LSA packets, ranging from 1 to 3600, with the default as 1.

dead *seconds*: Specifies the neighbor dead time in seconds, ranging from 1 to 32768, with the default as 40. This value must equal to the **dead** *seconds* configured on the virtual link peer router, and at least four times the value of **hello** *seconds*.

instance *Instance-id*: The instance ID of an virtual link, in the range of 0 to 255, with the default as 0.

Description Use the **vlink-peer** command to create and configure a virtual link.

Use the **undo vlink-peer** command to remove a virtual link.

For a non-backbone area without direct connection with the backbone area or for a backbone area that cannot maintain connectivity, you can use the **vlink-peer** command to create logical connectivity. A virtual link can be considered as an interface with OSPFv3 enabled, because parameters such as **hello**, **dead**, **retransmit** and **trans-delay** are configured in the similar way.

Both ends of a virtual link are ABRs that are configured with the **vlink-peer** command.

Examples # Create a virtual link to 10.110.0.3.

```
<Sysname> system-view
[Sysname] ospfv3 1
[Sysname-ospfv3-1] area 10.0.0.0
[Sysname-ospfv3-1-area-10.0.0.0] vlink-peer 10.110.0.3
```

85 IPv6 RIPng Configuration Commands

checkzero

Syntax **checkzero**

undo checkzero

View RIPng view

Parameters None

Description Use the **checkzero** command to enable the zero field check on RIPng packets.

Use the **undo checkzero** command to disable the zero field check.

The zero field check is enabled by default.

Some fields in RIPng packet headers must be zero. These fields are called zero fields. You can enable the zero field check on RIPng packet headers. If any such field contains a non-zero value, the RIPng packet will be discarded.

Examples # Disable the zero field check on RIPng packet headers of RIPng 100.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] undo checkzero
```

default cost (RIPng view)

Syntax **default cost** *cost*

undo default cost

View RIPng view

Parameters *cost*: Default metric of redistributed routes, in the range of 0 to 16.

Description Use the **default cost** command to specify the default metric of redistributed routes.

Use the **undo default cost** command to restore the default.

By default, the default metric of redistributed routes is 0.

The specified default metric applies to routes redistributed by the **import-route** command that has no metric specified.

Related commands: **import-route**.

Examples # Set the default metric of redistributed routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] default cost 2
```

display ripng

Syntax **display ripng** [*process-id*]

View Any view

Parameters *process-id*: RIPng process number, in the range of 1 to 65535.

Description Use the **display ripng** command to display the running status and configuration information of a RIPng process. If *process-id* is not specified, information of all RIPng processes will be displayed.

Examples # Display the running status and configuration information of all configured RIPng processes.

```
<Sysname> display ripng
    RIPng process : 1
       Preference : 100
       Checkzero : Enabled
       Default Cost : 0
       Maximum number of balanced paths : 3
       Update time  :   30 sec(s)  Timeout time           :  180 sec(s)
       Suppress time    :  120 sec(s)  Garbage-Collect time :  120 sec(s)
       Number of periodic updates sent : 0
       Number of trigger updates sent : 0
```

Table 316 Description on the fields of the display ripng command

Field	Description
RIPng Process	RIPng process number
Preference	RIPng route priority
Checkzero	Whether zero field check for RIPng packet headers is enabled
Default Cost	Default metric of redistributed routes
Maximum number of balanced paths	Maximum number of load balanced routes
Update time	RIPng updating interval, in seconds
Timeout time	RIPng timeout interval, in seconds
Suppress time	RIPng suppress interval, in seconds
Garbage-Collect time	RIPng garbage collection interval, in seconds

Table 316 Description on the fields of the display ripng command

Field	Description
Number of periodic updates sent	Number of periodic updates sent
Number of trigger updates sent	Number of triggered updates sent

display ripng database

Syntax **display ripng** *process-id* **database**

View Any view

Parameters *process-id*: RIPng process number, in the range of 1 to 65535.

Description Use the **display ripng database** command to display all active routes in the RIPng advertising database, which are sent in normal RIPng update messages.

Examples # Display the active routes in the database of RIPng process 100.

```
<Sysname> display ripng 100 database
   2001:7B::2:2A1:5DE/64,
        cost 4, Imported
   1:13::/120,
        cost 4, Imported
   1:32::/120,
        cost 4, Imported
   1:33::/120,
        cost 4, Imported
   100::/32,
       via FE80::200:5EFF:FE04:3302, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:1::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   3FFE:C00:C18:2::/64,
       via FE80::200:5EFF:FE04:B602, cost 2
   3FFE:C00:C18:3::/64,
       via FE80::200:5EFF:FE04:B601, cost 2
   4000:1::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
   4000:2::/64,
       via FE80::200:5EFF:FE04:3302, cost 2
```

Table 317 Description on fields of the display ripng database command

Field	Description
2001:7B::2:2A1:5DE/64	IPv6 destination address/prefix length
via	Next hop IPv6 address
cost	Route metric value
Imported	Routes learnt from other routing protocols

display ripng interface

Syntax **display ripng** *process-id* **interface** [*interface-type interface-number*]

View Any view

Parameters *process-id*: RIPng process number, in the range of 1 to 65535.

interface-type interface-number: Specified an interface.

Description Use the **display ripng interface** command to display the interface information of the RIPng process.

If no interface is specified, information about all interfaces of the RIPng process will be displayed.

Examples # Display the interface information of RIPng process 1.

```
<Sysname> display ripng 1 interface
Interface-name: Ethernet1/0
          Link Local Address: FE80::20F:E2FF:FE30:C16C
          Split-horizon: on             Poison-reverse: off
          MetricIn: 0                      MetricOut: 1
          Default route: off
          Summary address:
                 3:: 64
                 3:: 16
```

Table 318 Description on the fields of the display ripng interface command

Field	Description
Interface-name	Name of an interface running RIPng.
Link Local Address	Link-local address of an interface running RIPng
Split-horizon	Indicates whether the split horizon function is enabled (on: Enabled off: Disabled).
Poison-reverse	Indicates whether the poison reverse function is enabled (on: Enabled off: Disabled).
MetricIn/MetricOut	Additional metric to incoming and outgoing routes
Default route	■ Only/Originate: Only means that the interface advertises only default route. Originate means that the default route and other RIPng routes are advertised. ■ Off, indicates that no default route is advertised or the garbage-collect time expires after the default route advertisement was disabled. ■ In garbage-collect status: With default route advertisement disabled, the interface advertises the default route with metric 16 during the garbage-collect time.
Summary address	The summarized IPv6 prefix and the summary IPv6 prefix on the interface

display ripng route

Syntax **display ripng** *process-id* **route**

View Any view

Parameters *process-id*: RIPng process number, in the range of 1 to 65535.

Description Use the **display ripng route** command to display all RIPng routes and timers associated to each route of a RIPng process.

Examples # Display the routing information of RIPng process 100.

```
<Sysname> display ripng 100 route
   Route Flags: A - Aging, S - Suppressed, G - Garbage-collect
 ----------------------------------------------------------------
 Peer FE80::200:5EFF:FE04:B602  on Ethernet1/0
 Dest 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec
 Dest 3FFE:C00:C18:2::/64,
     via FE80::200:5EFF:FE04:B602, cost  2, tag 0, A, 34 Sec

 Peer FE80::200:5EFF:FE04:B601 on Ethernet1/1
 Dest 3FFE:C00:C18:1::/64,
     via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec
 Dest 3FFE:C00:C18:3::/64,
     via FE80::200:5EFF:FE04:B601, cost  2, tag 0, A, 13 Sec

 Peer FE80::200:5EFF:FE04:3302  on Ethernet1/2
 Dest 100::/32,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:1::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:2::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:3::/64,
     via FE80::200:5EFF:FE04:3302, cost  2, tag 0, A, 6 Sec
 Dest 4000:4::/64,
```

Table 319 Description on the fields of the display ripng route command

Field	Description
Peer	Neighbor connected to the interface
Dest	IPv6 destination address
via	Next hop IPv6 address
cost	Routing metric value
tag	Route tag
Sec	Time that a route entry stays in a particular state
A"	The route is in the aging state
S"	The route is in the suppressed state
G"	The route is in the Garbage-collect state

filter-policy export

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **export** [*protocol* [*process-id*]]

undo filter-policy export [*protocol* [*process-id*]]

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter advertised routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 prefix list used to filter routing information, a string of 1 to 19 characters.

protocol: Routing protocol from which to filter routes redistributed, currently including **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, and **static**

process-id: Process number of the specified routing protocol, in the range of 1 to 65535. This argument is specified only when the routing protocol is **rip**, **ospf**, or **isis**.

Description Use the **filter-policy export** command to define an outbound route filtering policy. Only routes passing the filter can be advertised in the update messages.

Use the **undo filter-policy export** command to restore the default.

By default, RIPng does not filter any outbound routing information.

With the *protocol* argument specified, only routing information redistributed from the specified routing protocol will be filtered. Otherwise, all routing information will be filtered.

Examples # Use IPv6 prefix list Filter 2 to filter advertised RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter2 export
```

filter-policy import (RIPng view)

Syntax **filter-policy** { *acl6-number* | **ipv6-prefix** *ipv6-prefix-name* } **import**

undo filter-policy import

View RIPng view

Parameters *acl6-number*: Specifies the number of an ACL to filter received routing information, in the range of 2000 to 3999.

ipv6-prefix *ipv6-prefix-name*: Specifies the name of an IPv6 Prefix list to filter incoming routes, in the range 1 to 19 characters.

Description Use the **filter-policy import** command to filter incoming routing information. Only routes which match the filtering policy can be received.

Use the **undo filter-policy import** command to disable incoming route filtering.

By default, RIPng does not filter incoming routing information.

Examples # Reference IPv6 prefix list **Filter1** to filter received RIPng updates.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] filter-policy ipv6-prefix Filter1 import
```

import-route

Syntax **import-route** *protocol* [*process-id*] [**allow-ibgp**] [**cost** *cost* | **route-policy** *route-policy-name*] *

undo import-route *protocol* [*process-id*]

View RIPng view

Parameters *protocol*: Specifies a routing protocol from which to redistribute routes. Currently, it can be **bgp4+**, **direct**, **isisv6**, **ospfv3**, **ripng**, or **static**.

process-id: Process ID, in the range of 1 to 65535. The default is 1. This argument is available only when the protocol is **isisv6**, **ospfv3**, or **ripng**.

cost: Routing metric of redistributed routes, in the range of 0 to 16. If *cost value* is not specified, the metric is the default metric specified by the **default cost** command.

route-policy *route-policy-name*: Specifies a routing policy by its name with 1 to 19 characters.

allow-ibgp: Optional keyword when the specified *protocol* is **bgp4+**. The **import-route bgp4+** command redistributes only EBGP routes. The **import-route bgp4+ allow-ibgp** command redistributes additionally IBGP routes, thus be cautious when using it.

Description Use the **import-route** command to redistribute routes from another routing protocol.

Use the **undo import-route** command to disable redistributing routes from another routing protocol.

By default, RIPng does not redistribute routes from other routing protocols.

- You can configure a routing policy to redistribute only needed routes.
- You can specify a cost for redistributed routes using keyword **cost**.

Related commands: **default cost** on page 1280.

Examples # Redistribute IPv6-IS-IS routes (process 7) and specify the metric as 7.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] import-route isisv6 7 cost 7
```

maximum load-balancing (RIPng view)

Syntax **maximum load-balancing** *number*

undo maximum load-balancing

View RIPng view

Parameters *number*: Maximum number of equal-cost load-balanced routes, in the range 1 to 8.

Description Use the **maximum load-balancing** command to specify the maximum number of equal cost routes for load balancing.

Use the **undo maximum load-balancing** command to restore the default.

You need configure the maximum number according to the memory size.

Examples # Set the maximum number of equal cost load balanced routes to 2.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] maximum load-balancing 2
```

Restore the default.

```
[Sysname-ripng-100] undo maximum load-balancing
```

preference

Syntax **preference** [**route-policy** *route-policy-name*] *preference*

undo preference [**route-policy**]

View RIPng view

Parameters *route-policy-name*: Name of a routing policy, in the range of 1 to 19 characters.

preference: RIPng route priority, in the range of 1 to 255.

Description

Use the **preference** command to specify the RIPng route priority.

Use the **undo preference route-policy** command to restore the default.

By default, the priority of a RIPng route is 100.

Using the **route-policy** keyword can set a priority for routes filtered in by the routing policy:

- If a priority is set in the routing policy, the priority applies to matched routes, and the priority set by the **preference** command applies to routes not matched.
- If no priority is set in the routing policy, the one set by the **preference** command applies to all routes.

Examples

Set the RIPng route priority to 120.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] preference 120
```

Restore the default RIPng route priority.

```
[Sysname-ripng-100] undo preference
```

ripng

Syntax

ripng [*process-id*]

undo ripng [*process-id*]

View

System view

Parameters

process-id: RIPng process number, in the range of 1 to 65535. The default value is 1.

Description

Use the **ripng** command to create a RIPng process and enter RIPng view.

Use the **undo ripng** command to disable a RIPng process.

By default, no RIPng process is enabled.

Examples

Create RIPng process 100 and enter its view.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100]
```

Disable RIPng process 100.

```
[Sysname] undo ripng 100
```

ripng default-route

Syntax **ripng default-route** { **only** | **originate** } [**cost** *cost*]

undo ripng default-route

View Interface view

Parameters **only**: Indicates that only the IPv6 default route (::/0) is advertised via the interface.

originate: Indicates that the IPv6 default route (::/0) is advertised without suppressing other routes.

cost: Metric of the advertised default route, in the range of 1 to 15, with a default value of 1.

Description Use the **ripng default-route** command to advertise a default route with the specified routing metric to a RIPng neighbor.

Use the **undo ripng default-route** command to stop advertising and forwarding the default route.

By default, a RIP process does not advertise any default route.

After you execute this command, the generated RIPng default route is advertised in a route update over the specified interface. This IPv6 default route is advertised without considering whether it already exists in local IPv6 routing table.

Examples # Advertise only the default route via Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng default-route only
```

Advertise the default route together with other routes via Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng default-route originate
```

ripng enable

Syntax **ripng** *process-id* **enable**

undo ripng enable

View Interface view

Parameters *process-id*: RIPng process number, in the range of 1 to 65535.

Description Use the **ripng enable** command to enable RIPng on the specified interface.

Use the **undo ripng enable** command to disable RIPng on the specified interface.

By default, RIPng is disabled on an interface.

Examples # Enable RIPng100 on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng 100 enable
```

ripng metricin

Syntax **ripng metricin** *value*

undo ripng metricin

View Interface view

Parameters *value*: Additional metric to received routes, in the range of 0 to 16.

Description Use the **ripng metricin** command to specify an additional metric for received RIPng routes.

Use the **undo ripng metricin** command to restore the default.

By default, the additional metric to received routes is 0.

Related commands: **ripng metricout**.

Examples # Specify the additional routing metric as 12 for RIPng routes received by Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng metricin 12
```

ripng metricout

Syntax **ripng metricout** *value*

undo ripng metricout

View Interface view

Parameters *value*: Additional metric to advertised routes, in the range of 1 to 16.

Description Use the **ripng metricout** command to configure an additional metric for RIPng routes advertised by an interface.

Use the **undo rip metricout** command to restore the default.

The default additional routing metric is 1.

Related commands: **ripng metricin**.

Examples # Set the additional metric to 12 for routes advertised by Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng metricout 12
```

ripng poison-reverse

Syntax **ripng poison-reverse**

undo ripng poison-reverse

View Interface view

Parameters None

Description Use the **rip poison-reverse** command to enable the poison reverse function.

Use the **undo rip poison-reverse** command to disable the poison reverse function.

By default, the poison reverse function is disabled.

Examples # Enable the poison reverse function for RIPng update messages on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng poison-reverse
```

ripng split-horizon

Syntax **ripng split-horizon**

undo ripng split-horizon

View Interface view

Parameters None

Description Use the **rip split-horizon** command to enable the split horizon function.

Use the **undo rip split-horizon** command to disable the split horizon function.

By default, the split horizon function is enabled.

Note that:

- The split horizon function is necessary for preventing routing loops. Therefore, you are not recommended to disable it.
- In special cases, make sure that it is necessary to disable the split horizon function before doing so.

- *If both the poison reverse and split horizon functions are enabled, only the poison reverse function takes effect.*
- *On Frame Relay, X.25 and other non-broadcast multi-access (NBMA) links, split horizon should be disabled if multiple VCs are configured on the primary interface and secondary interfaces to ensure route advertisement. For detailed information, refer to "Frame Relay Configuration Commands" on page 371 and "LAPB and X.25 Configuration Commands" on page 421.*

Examples # Enable the split horizon function on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ripng split-horizon
```

ripng summary-address

Syntax **ripng summary-address** *ipv6-address prefix-length*

undo ripng summary-address *ipv6-address prefix-length*

View Interface view

Parameters *ipv6-address*: Destination IPv6 address of the summary route.

prefix-length: Prefix length of the destination IPv6 address of the summary route, in the range of 0 to 128. It indicates the number of consecutive 1s of the prefix, which defines the network ID.

Description Use the **ripng summary-address** command to configure a summary advertised through the interface.

Use the **undo ripng summary-address** command to remove the summary.

If the prefix and the prefix length of a route match the IPv6 prefix, the IPv6 prefix will be advertised instead. Thus, one route can be advertised on behalf of many routes. After summarization, the summary route cost is the lowest cost among summarized routes.

Examples # Assign an IPv6 address with the 64-bit prefix to Ethernet1/0 and configure a summary with the 35-bit prefix.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipv6 address 2001:200::3EFF:FE11:6770/64
[Sysname-Ethernet1/0] ripng summary-address 2001:200:: 35
```

timers

Syntax **timers** { **garbage-collect** *garbage-collect-value* | **suppress** *suppress-value* | **timeout** *timeout-value* | **update** *update-value* }*

undo timers { **garbage-collect** | **suppress** | **timeout** | **update** }*

View RIPng view

Parameters *garbage-collect-value*: Interval of the garbage-collect timer in seconds, in the range of 1 to 86400.

suppress-value: Interval of the suppress timer in seconds, in the range of 0 to 86400.

timeout-value: Interval of the timeout timer in seconds, in the range of 1 to 86400.

update-value: Interval of the update timer in seconds, in the range of 1 to 86400.

Description Use the **timers** command to configure RIPng timers.

Use the **undo timers** command to restore the default.

By default, the garbage-collect timer is 120 seconds, the suppress timer 120 seconds, the timeout timer 180 seconds, and the update timer 30 seconds.

RIPng is controlled by the above four timers.

- The update timer defines the interval between update messages.
- The timeout timer defines the route aging time. If no update message related to a route is received within the aging time, the metric of the route is set to 16 in the routing table.
- The suppress timer defines how long a RIPng route stays in the suppressed state. When the metric of a route is 16, the route enters the suppressed state. In the suppressed state, only routes which come from the same neighbor and whose metric is less than 16 will be received by the router to replace unreachable routes.
- The garbage-collect timer defines the interval from when the metric of a route becomes 16 to when it is deleted from the routing table. During the garbage-collect timer length, RIPng advertises the route with the routing metric set to 16. If no update message is announced for that route before the

garbage-collect timer expires, the route will completely be deleted from the routing table.

Note that:

- You are not recommended to change the default values of these timers under normal circumstances.
- The lengths of these timers must be kept consistent on all routers and access servers in the network

Examples # Configure the update, timeout, suppress, and garbage-collect timers as 5s, 15s, 15s and 30s.

```
<Sysname> system-view
[Sysname] ripng 100
[Sysname-ripng-100] timers update 5
[Sysname-ripng-100] timers timeout 15
[Sysname-ripng-100] timers suppress 15
[Sysname-ripng-100] timers garbage-collect 30
```

86 IPv6 Static Routing Configuration Commands

delete ipv6 static-routes all

Syntax **delete ipv6 static-routes all**

View System view

Parameters None

Description Use the **delete ipv6 static-routes all** command to delete all static routes including the default route.

When using this command, you will be prompted whether to continue the deletion and only after you confirm the deletion will the static routes be deleted.

Related commands: **display ipv6 routing-table** on page 942 and **ipv6 route-static**.

Examples # Delete all IPv6 static routes.

```
<Sysname> system-view
[Sysname] delete ipv6 static-routes all
This will erase all ipv6 static routes and their configurations, you
 must reconfigure all static routes
Are you sure?[Y/N]Y
```

ipv6 route-static

Syntax For a broadcast interface (Ethernet interface, VLAN interface), or NBMA interface (X25 or frame relay interface):

ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] *nexthop-address* [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number*] [*nexthop-address*] [**preference** *preference-value*]

For a point-to-point interface (serial port):

ipv6 route-static *ipv6-address prefix-length* { *interface-type interface-number* | *nexthop-address* } [**preference** *preference-value*]

undo ipv6 route-static *ipv6-address prefix-length* [*interface-type interface-number* | *nexthop-address*] [**preference** *preference-value*]

View System view

Parameters *ipv6-address prefix-length*: IPv6 address and prefix length.

interface-type interface-number: Interface type and interface number of the output interface.

nexthop-address: Next hop IPv6 address.

preference-value: Route preference value, in the range of 1 to 255. The default is 60.

Description Use the **ipv6 route-static** command to configure an IPv6 static route.

Use the **undo ipv6 route-static** command to remove an IPv6 static route.

An IPv6 static route that has the destination address configured as "::/0" (a prefix length of 0) is the default IPv6 route. If the destination address of an IPv6 packet does not match any entry in the routing table, this default route will be used to forward the packet.

While configuring static routes, you can configure either the output interface or the next-hop address depending on the situations:

- If the output interface is a broadcast interface, such as an Ethernet interface, a VLAN interface, or an NBMA interface (such as an interface with X25 or frame relay encapsulated), then the next hop address must be specified;
- If the output interface is a point-to-point interface, such as a serial port, you can specify either the output interface or the next hop address, but not both.

Related commands: **display ipv6 routing-table** on page 942 and **delete ipv6 static-routes all**.

Examples # Configure a static IPv6 route, with the destination address being 1:1:2::/24 and next hop being 1:1:3::1.

```
<Sysname> system-view
[Sysname] ipv6 route-static 1:1:2:: 24 1:1:3::1
```

87 MULTICAST ROUTING AND FORWARDING CONFIGURATION COMMANDS

display multicast boundary

Syntax **display multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **boundary** [*group-address* [*mask* | *mask-length*]] [**interface** *interface-type interface-number*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group address, in the range of 4 to 32. The system default is 32.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **display multicast boundary** command to view the multicast boundary information on the specified interface or all interfaces.

Related command: **multicast boundary**.

Example # View the multicast boundary information on all interfaces in the public instance.

```
<Sysname> display multicast boundary
Multicast boundary information of VPN-Instance: public net
 Boundary            Interface
 224.1.1.0/24        Eth1/0
 239.2.2.0/24        Pos5/0
```

Table 320 Description on the fields of the display multicast boundary command

Field	Description
Boundary	Multicast group corresponding to the multicast boundary
Interface:	Boundary interface corresponding to the multicast boundary

display multicast forwarding-table

Syntax **display multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics**] * [**port-info**]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays forwarding entries of which the incoming interface is the specified one.

register: Specifies the register interface.

outgoing-interface: Displays forwarding entries of which the outgoing interface is the specified one.

exclude: Displays the routing entries of which the outgoing interface list (OIL) excludes the specified interface.

include: Displays the routing entries of which the OIL includes the specified interface.

match: Specifies the routing entries of which the OIL includes and includes only the specified interface.

statistics: Specifies to display the statistics information of the multicast forwarding table.

port-info: Specifies to display Layer 2 port information.

Description Use the **display multicast forwarding-table** command to view the multicast forwarding table information.

Related command: **multicast forwarding-table downstream-limit**, **multicast forwarding-table route-limit** and **display multicast routing-table**.

Example # View the multicast forwarding table information in the public network instance.

```
<Sysname> display multicast forwarding-table
Multicast Forwarding Table of VPN-Instance: public net
Total 1 entry

Total 1 entry matched

00001. (172.168.0.2, 227.0.0.1)
     MID: 0, Flags: 0x0:0
     Uptime: 00:08:32, Timeout in: 00:03:26
     Incoming interface: Ethernet1/0
     List of 1 outgoing interfaces:
       1: Ethernet1/1
     Matched 19648 packets(20512512 bytes), Wrong If 0 packets
     Forwarded 19648 packets(20512512 bytes)
```

Table 321 Description on the fields of display multicast forwarding-table

Field	Description
00001	Sequence number of the (S, G) entry
(172.168.0.2,227.0.0.1)	An (S, G) entry of the multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has a unique MID
Flags	Current state of the (S, G) entry. Different bits are used to indicate different states of (S, G) entries. Major values of this field are described in Table 322.
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds
Timeout in	Length of time in which the (S, G) entry will expire, in hours:minutes:seconds
Incoming interface	Incoming interface of the (S, G) entry
List of outgoing interface:	1 outgoing interface list:
1: Ethernet1/1	Sequence number of outgoing interface: outgoing interface type and number
Matched 19648 packets (20512512 bytes), Wrong If 0 packets	Number of matched packets (number of bytes), number of packets with incoming interface errors
Forwarded 19648 packets (20512512 bytes)	Number of forwarded packets (number of bytes)

Table 322 Major values of the flags field

Value	Meaning
0x00000001	Indicates that a register-stop message must be sent
0x00000002	Indicates whether the multicast source corresponding to the (S, G) is active
0x00000004	Indicates a null forwarding entry
0x00000008	Indicates whether the RP is a PIM domain border router
0x00000010	Indicates that a register outgoing interface is available
0x00000400	Identifies an entry to be deleted

Table 322 Major values of the flags field

Value	Meaning
0x00008000	Indicates that the (S, G) entry is in the smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) has been updated during the smoothing process
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and needs to be deleted before a new entry is added
0x00100000	Indicates that an entry is successfully added

display multicast minimum-ttl

Syntax **display multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **minimum-ttl** [*interface-type interface-number*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

interface-type interface-number: Specifies an interface by its type and number. If you do not specify an interface, this command will display the minimum time-to-live (TTL) required for a multicast packet to be forwarded on all interfaces.

Description Use the **display multicast minimum-ttl** command to view the minimum TTL required for a multicast packet to be forwarded on the specified interface or all interfaces.

Related command: **multicast minimum-ttl**.

Example # View the minimum TTL required for a multicast packet to be forwarded on all interfaces of the public instance.

```
<Sysname> display multicast minimum-ttl
Multicast TTL information of VPN-Instance: public net
 Interface           TTL
 Eth1/0              5
 Eth1/1              6
```

Table 323 Description on the fields of the display multicast minimum-ttl command

Field	Description
Interface	Interface name
TTL	Minimum TTL required for a multicast packet to be forwarded on the interface

display multicast routing-table

Syntax **display multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Displays multicast routing entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface of PIM-SM.

outgoing-interface: Displays multicast routing entries of which the outgoing interface is the specified one.

exclude: Displays routing entries of which the OIL excludes the specified interface.

include: Displays routing entries of which the OIL includes the specified interface.

match: Displays routing entries of which the OIL includes only the specified interface.

Description Use the **display multicast routing-table** command to view the multicast routing table information.

Related command: **display multicast forwarding-table**.

Example # View the routing information in the multicast routing table of the public instance.

```
<Sysname> display multicast routing-table
Multicast routing table of VPN-Instance: public net
 Total 1 entry
 00001. (172.168.0.2, 227.0.0.1)
       Uptime: 00:00:28
       Upstream Interface: Ethernet1/1
       List of 2 downstream interfaces
           1:  Ethernet1/2
           2:  Ethernet1/0
```

Table 324 Description on the fields of display multicast routing-table

Field	Description
00001	Sequence number of the (S, G) entry
(172.168.0.2, 227.0.0.1)	An (S, G) entry of the multicast forwarding table
Uptime	Length of time for which the (S, G) entry has been up, in hours:minutes:seconds
Upstream interface	Upstream interface the (S, G) entry: multicast packets should arrive at this interface
List of 2 downstream interfaces	Downstream interface list: these interfaces need to forward multicast packets

display multicast routing-table static

Syntax **display multicast routing-table** [**vpn-instance** *vpn-instance-name* | **all-instance**] **static** [**config**] [*source-address* { *mask-length* | *mask* }]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

config: Displays the configuration information of static routes.

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

Description Use the **display multicast routing-table static** command to view the information of multicast static routes.

Example # View all the multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static
Multicast Routing Table of VPN-Instance: public net
Routes : 1

 Mroute 10.10.0.0/16
          Interafce = Ethernet1/0         RPF Neighbor = 10.10.0.254
          Matched routing protocol = <none>, Route-policy = <none>
```

```
          Preference = 1, Order = 1
 Running Configuration = ip rpf-route-static 10.10.0.0 16 2.2.2.2 order 1
```

View the configuration information of multicast static routes in the public instance.

```
<Sysname> display multicast routing-table static config

Multicast Routing Table of VPN-Instance: public net
Routes : 1

 Mroute 10.10.0.0/16,      interface = Ethernet1/0
 Matched routing protocol = <none>, Route-policy = <none>
 Preference = 1, Order = 1
```

Table 325 Description on the fields of display multicast routing-table static

Field	Description
Mroute	Multicast route source address and its mask length
Interface	Outgoing interface to the multicast source
RPF Neighbor	IP address of an RPF neighbor through which the multicast source is reachable
Matched routing protocol	If a protocol is configured, the multicast source address of the route should be the destination address of an entry in unicast routing table
Route-policy	Routing policy. The multicast source address of the route should match the routing policy
Preference	Route preference
Order	Sequence number of the route

display multicast rpf-info

Syntax **display multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **rpf-info** *source-address* [*group-address*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

Description Use the **display multicast rpf-info** command to view the RPF information of a multicast source.

Related command: **display multicast routing-table** and **display multicast forwarding-table**.

Example # View all the RPF information of multicast source 192.168.1.55 in the public network.

```
<Sysname> display multicast rpf-info 192.168.1.55
RPF information about source 192.168.1.55:
     RPF interface: Ethernet1/0, RPF neighbor: 10.1.1.1
     Referenced route/mask: 192.168.1.0/24
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 326 Description on the fields of the display multicast rpf-info command

Field	Description
RPF information about source 192.168.1.55	Information of the RPF path to multicast source 192.168.1.55
RPF interface	RPF interface
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Referenced route and its mask length
Referenced route type	Type of the referenced route, which can be any of the following: ■ igp: unicast route (IGP) ■ egp: unicast route (BGP) ■ unicast (direct): unicast route (directly connected) ■ unicast: other unicast route (such as unicast static route) ■ multicast static: multicast static route
Route selection rule	Rule for RPF route selection, which can be based on the preference of the routing protocol or based on the longest match on the destination address
Load splitting rule	Status of the load splitting rule (enabled/disabled)

ip rpf-route-static

Syntax **ip rpf-route-static** [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*] { *rpf-nbr-address* | *interface-type interface-number* } [**preference** *preference*] [**order** *order-number*]

undo ip rpf-route-static [**vpn-instance** *vpn-instance-name*] *source-address* { *mask* | *mask-length* } [*protocol* [*process-id*]] [**route-policy** *policy-name*]

View System view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

source-address: Multicast source address.

mask: Mask of the multicast source address.

mask-length: Mask length of the multicast source address, in the range of 0 to 32.

protocol: Routing protocol, which can have any of the following values:

- **bgp**: Specifies the BGP protocol
- **isis**: Specifies the IS-IS protocol
- **ospf**: Specifies the OSPF protocol
- **rip**: Specifies the RIP protocol

process-id: Process number of the unicast routing protocol, in the range of 1 to 65535. This argument must be provided if IS-IS, OSPF or RIP is the specified unicast routing protocol.

policy-name: Name of the multicast route match rule, a case sensitive string of up to 19 characters.

rpf-nbr-address: IP address of the PPF neighbor.

interface-type interface-number: Specifies the interface type and number of an RPF neighbor. The interface type must not be Ethernet, GigabitEthernet, Loopback or Vlan-interface.

preference: Route preference, in the range of 1 to 255 and defaulting to 1.

order-number: Match order for routes on the same segment, in the range of 1 to 100.

Description Use the **ip rpf-route-static** command to configure a multicast static route.

Use the **undo ip rpf-route-static** command to delete a multicast static route from the multicast static routing table.

By default, no multicast static route is configured.

Note that:

- The arguments *source-address* { *mask* | *mask-length* }, *protocol* and *policy-name* are critical elements in multicast static route configuration. The variation of any of these three arguments results in a different configuration.
- In the configuration, you can use the **display multicast routing-table static** command to check whether the multicast static route information contains this configuration. If you find a match, modify the corresponding fields without changing the configuration sequence; otherwise, add a multicast static route.
- When configuring a multicast static route, you cannot designate an RPF neighbor by specifying an interface (by means of the *interface-type interface-number* command argument combination) if the interface type of that router is Ethernet, GigabitEthernet, Loopback or Vlan-interface; instead, you can designate an RPF neighbor only by specifying an address (*rpf-nbr-address*).
- Because outgoing interface iteration may fail or the specified interface may be in the down state, the multicast static route configured with this command may fail to take effect. Therefore, we recommend that you use the **display multicast routing-table static** command after you configure a multicast

static route to check whether the route has been successfully configured or whether the route has taken effect.

Related command: **display multicast routing-table static**.

Example # Configure a multicast static route to the multicast source 10.1.1.1/24, specifying a router with the IP address of 192.168.1.23 as its RPF neighbor.

```
<Sysname> system-view
[Sysname] ip rpf-route-static 10.1.1.1 24 192.168.1.23
```

mtracert

Syntax **mtracert** *source-address* [[*last-hop-router-address*] *group-address*]

View Any view

Parameters *source-address*: Specifies a multicast source address.

group-address: Specifies a multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

last-hop-router-address: Specifies a last-hop router address, which is the IP address of the local router by default.

Description Use the **mtracert** command to trace the path down which the multicast traffic from a given multicast source flows to the last-hop router.

Note that if the *last-hop-router-address* argument is given in the command to trace the path for a specific (S, G) multicast stream, the interface corresponding to the last-hop router address must be the outgoing interface for the (S, G) multicast stream; otherwise the multicast traceroute will fail.

Examples # Trace the path down which the (6.6.6.6, 225.2.1.1) multicast traffic flows from the multicast source to the last-hop router with the (S, G) outgoing interface address of 5.5.5.8.

```
<Sysname> mtracert 6.6.6.6 5.5.5.8 225.2.1.1
Type Ctrl+C to quit mtrace facility
Tracing reverse path of (6.6.6.6, 225.2.1.1) from last-hop router (5
.5.5.8) to source via multicast routing-table

 -1 5.5.5.8
   Incoming interface address: 4.4.4.8
   Previous-hop router address: 4.4.4.7
   Input packet count on incoming interface: 17837
   Output packet count on outgoing interface: 0
   Total number of packets for this source-group pair: 8000
   Protocol: PIM
   Forwarding TTL: 0
   Forwarding code: No error
```

```
-2 4.4.4.7
  Incoming interface address: 6.6.6.7
  Previous-hop router address: 0.0.0.0
  Input packet count on incoming interface: 2
  Output packet count on outgoing interface: 259
  Total number of packets for this source-group pair: 8100
  Protocol: PIM
  Forwarding TTL: 0
  Forwarding code: No error
```

Table 327 Description on the fields of the mtracert command

Field	Description
last-hop router	Last-hop router
(6.6.6.6, 225.2.1.1)	The (S, G) multicast stream for which the forwarding path is being traced
-1 5.5.5.8	The (S, G) outgoing interface address of each hop, starting from the last-hop router
Incoming interface address	The address of the interface on which the (S, G) packets arrive
Previous-hop router address	The IP address of the router from which this router receives packets from this source
Input packet count on incoming interface	The total number of multicast packets received on the incoming interface
Output packet count on outgoing interface	The total number of multicast packets transmitted for transmission on the outgoing interface
Total number of packets for this source-group pair	The total number of packets from the specified source forwarded by this router to the specified group
Protocol	The multicast routing protocol in use between this router and the previous hop router
Forwarding TTL	The minimum TTL that a packet is required to have before it can be forwarded over the outgoing interface
Forwarding code	Forwarding code

multicast boundary

Syntax **multicast boundary** *group-address* { *mask* | *mask-length* }

undo multicast boundary { *group-address* { *mask* | *mask-length* } | **all** }

View Interface view

Parameter *group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address, in the range of 4 to 32.

all: Specifies to remove all forwarding boundaries configured on the interface.

Description Use the **multicast boundary** command to configure a multicast forwarding boundary.

Use the **undo multicast boundary** command to remove a multicast forwarding boundary.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the multicast groups in the specified range. If the destination address of a multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related command: **display multicast boundary**.

Example # Configure Ethernet 1/0 to be the forwarding boundary of multicast group 239.2.0.0/16.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] multicast boundary 239.2.0.0 16
```

multicast forwarding-table downstream-limit

Syntax **multicast forwarding-table downstream-limit** *limit*

undo multicast forwarding-table downstream-limit

View System view, VPN instance view

Parameter *limit*: Maximum number of downstream nodes (namely, the maximum number of outgoing interfaces) for a single route in the multicast forwarding table. The value ranges from 0 to 128.

Description Use the **multicast forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single route in the multicast forwarding table.

Use the **undo multicast forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single route in the multicast forwarding table is 128.

The system-allowed maximum number varies with different device models. Refer to your specific device model.

Related command: **display multicast forwarding-table**.

Example # Set the maximum number of downstream nodes for a single route in the multicast forwarding table of the public instance to 120.

```
<Sysname> system-view
[Sysname] multicast forwarding-table downstream-limit 120
```

Set the maximum number of downstream nodes for a single route in the multicast forwarding table of VPN instance mvpn to 60.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast forwarding-table downstream-limit 60
```

multicast forwarding-table route-limit

Syntax **multicast forwarding-table route-limit** *limit*

undo multicast forwarding-table route-limit

View System view, VPN instance view

Parameter *limit*: Maximum number of route entries in the multicast forwarding table. The value ranges from 0 to 900.

Description Use the **multicast forwarding-table route-limit** command to configure the maximum number of route entries in the multicast forwarding table.

Use the **undo multicast forwarding-table route-limit** command to restore the system default.

By default, the maximum number of route entries in the multicast forwarding table is 900.

The system-allowed maximum number varies with different device models. Refer to your specific device model.

Related command: **display multicast forwarding-table**.

Example # Set the maximum number of routing entries in the multicast forwarding table of the public instance to 200.

```
<Sysname> system-view
[Sysname] multicast forwarding-table route-limit 200
```

Set the maximum number of routing entries in the multicast forwarding table of VPN instance mvpn to 200.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast forwarding-table route-limit 200
```

multicast load-splitting

Syntax **multicast load-splitting** { **source** | **source-group** }

undo multicast load-splitting

View System view, VPN instance view

Parameter **source**: Specifies to implement per-source load splitting.

source-group: Specifies to implement per-source and per-group load splitting simultaneously.

Description Use the **multicast load-splitting** command to enable load splitting of multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of multicast traffic.

By default, load splitting of multicast traffic is disabled.

Example # Enable per-source load splitting of multicast traffic in the public instance.

```
<Sysname> system-view
[Sysname] multicast load-splitting source
```

Enable per-source load splitting of multicast traffic in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast load-splitting source
```

multicast longest-match

Syntax **multicast longest-match**

undo multicast longest-match

View System view, VPN instance view

Parameter None

Description Use the **multicast longest-match** command to configure route selection based on the longest match, namely based on the mask length.

Use the **undo multicast longest-match** command to remove the configuration of route selection based on the longest match.

By default, routes are selected according to the order of route entries.

Example # Configure route selection based on the longest match in the public instance.

```
<Sysname> system-view
[Sysname] multicast longest-match
```

Configure route selection based on the longest match in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast longest-match
```

multicast minimum-ttl

Syntax **multicast minimum-ttl** *ttl-value*

undo multicast minimum-ttl

View Interface view

Parameter *ttl-value*: Minimum TTL required for a multicast packet to be forwarded on the interface, in the range of 1 to 255.

Description Use the **multicast minimum-ttl** command to configure the minimum TTL required for a multicast packet to be forwarded on the interface.

Use the **undo multicast minimum-ttl** command to restore the system default.

By default, the minimum TTL value required for a multicast packet to be forwarded is 1.

Related command: **display multicast minimum-ttl**.

Example # Set the minimum TTL required for a multicast packet to be forwarded on Ethernet 1/0 to 8.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] multicast minimum-ttl 8
```

multicast routing-enable

Syntax **multicast routing-enable**

undo multicast routing-enable

View System view, VPN instance view

Parameter None

Description Use the **multicast routing-enable** command to enable IP multicast routing.

Use the **undo multicast routing-enable** command to disable IP multicast routing.

IP multicast routing is disabled by default.

Note that:

- You must enable IP multicast routing in the public instance or VPN instance before you can carry out other Layer 3 multicast commands in the corresponding instance.
- The device does not forward any multicast packets before IP multicast routing is enabled.

Example # Enable IP multicast routing in the public instance.

```
<Sysname> system-view
[Sysname] multicast routing-enable
```

Enable IP multicast routing in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
```

reset multicast forwarding-table

Syntax **reset multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **forwarding-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Specifies to clear multicast forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface of PIM-SM.

all: Specifies to clear all the forwarding entries from the multicast forwarding table.

Description Use the **reset multicast forwarding-table** command to clear the multicast forwarding table information.

When a forwarding entry is deleted from the multicast forwarding table, the corresponding route entry is also deleted from the multicast routing table.

Related command: **reset multicast routing-table**, **display multicast routing-table**, and **display multicast forwarding-table**.

Example # Clear the multicast forwarding entries related to multicast group 225.5.4.3 from the multicast forwarding table of the public instance.

```
<Sysname> reset multicast forwarding-table 225.5.4.3
```

Clear the multicast forwarding entries related to multicast group 226.1.2.3 from the multicast forwarding table of VPN instance mvpn.

```
<Sysname> reset multicast vpn-instance mvpn forwarding-table 226.1.2.3
```

reset multicast routing-table

Syntax **reset multicast** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** { { *source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for a

multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

incoming-interface: Specifies the incoming interface of multicast routing entries.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface.

all: Specifies to clear all the routing entries from the multicast routing table.

Description Use the **reset multicast routing-table** command to clear multicast routing entries from the multicast routing table.

When a route entry is deleted from the multicast routing table, the corresponding forwarding entry is also deleted from the multicast forwarding table.

Related command: **reset multicast forwarding-table**, **display multicast routing-table** and **display multicast forwarding-table**.

Example # Clear the route entries related to multicast group 225.5.4.3 from the multicast routing table of the public instance.

```
<Sysname> reset multicast routing-table 225.5.4.3
```

Clear the route entries related to multicast group 226.1.2.3 from the multicast routing table of VPN instance mvpn.

```
<Sysname> reset multicast vpn-instance mvpn routing-table 226.1.2.3
```

88 IGMP CONFIGURATION COMMANDS

display igmp group

Syntax **display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** [*group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

interface *interface-type interface-number*: Displays the IGMP multicast group information about a particular interface.

static: Displays the information of statically joined IGMP multicast groups.

verbose: Displays the detailed information of IGMP multicast groups.

Description Use the **display igmp group** command to view IGMP multicast group information.

Note that:

- If you do not specify *group-address*, this command will display the IGMP information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the IGMP multicast group information on all the interfaces.
- If you do not specify the **static** keyword, this command will display the detailed information about the dynamically joined IGMP multicast groups.

Example # Display the information about dynamically joined IGMP multicast groups on all interfaces in the public instance.

```
<Sysname> display igmp group
Total 3 IGMP Group(s).
Interface group report information of VPN-Instance: public net
 Ethernet1/0(20.20.20.20):
  Total 3 IGMP Groups reported
```

```
  Group Address   Last Reporter   Uptime      Expires
  225.1.1.1       20.20.20.20     00:02:04    00:01:15
  225.1.1.3       20.20.20.20     00:02:04    00:01:15
  225.1.1.2       20.20.20.20     00:02:04    00:01:17
```

Display the detailed information of multicast group 225.1.1.1 in the public instance.

```
<Sysname> display igmp group 225.1.1.1 verbose
Interface group report information of VPN-Instance: public net
 Ethernet1/0(10.10.1.20):
  Total 1 IGMP Groups reported
   Group: 225.1.1.1
     Uptime: 00:00:34
     Expires: 00:00:40
     Last reporter: 10.10.1.10
     Last-member-query-counter: 0
     Last-member-query-timer-expiry: off
     Version1-host-present-timer-expiry: off
```

Table 328 Description on the fields of the display igmp group command

Field	Description
Group	Multicast group address
Uptime	Length of time since the multicast group was reported
Expires	Remaining time of the multicast group
Last reporter	Address of the last host that reported its membership for this multicast group
Last-member-query-counter	Number of group-specific queries sent
Last-member-query-timer-expiry	Remaining time of the last member query timer
Version1-host-present-timer-expiry	Remaining time of the IGMPv1 host present timer

display igmp interface

Syntax **display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

interface-type interface-number: Specifies an interface to display the IGMP configuration and operation information about. If no interface is specified, this command will display the related information of all IGMP-enabled interfaces.

verbose: Displays the detailed IGMP configuration and operation information.

Description Use the **display igmp interface** command to view IGMP configuration and operation information of the specified interface or all IGMP-enabled interfaces.

Example # View the detailed IGMP configuration and operation information on Ethernet 1/0 in the public interface.

```
<Sysname> display igmp interface ethernet 1/0 verbose
Ethernet1/0(10.10.1.20):
   IGMP is enabled
   Current IGMP version is 2
   Value of query interval for IGMP(in seconds): 60
   Value of other querier present interval for IGMP(in seconds): 125
   Value of maximum query response time for IGMP(in seconds): 10
   Value of last member query interval(in seconds): 1
   Value of startup query interval(in seconds): 15
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:54
   Querier for IGMP: 10.10.1.20 (this router)
   IGMP activity: 1 joins, 0 leaves
   Multicast routing on this interface: enabled
   Robustness: 2
   Require-router-alert: disabled
   Fast-leave: disabled
   Startup-query-timer-expiry: off
   Other-querier-present-timer-expiry: off
  Total 1 IGMP Group reported
```

Table 329 Description on the fields of the display igmp interface command

Field	Description
Ethernet1/0 (10.10.1.20)	Interface name (IP address)
Current IGMP version	Version of IGMP currently running on the interface
Value of query interval for IGMP(in seconds)	IGMP query interval, in seconds
Value of other querier present interval for IGMP(in seconds)	Other querier present interval, in seconds
Value of maximum query response time for IGMP(in seconds)	Maximum response time for IGMP general queries, in seconds
Value of last member query interval(in seconds)	IGMP last member query interval in seconds
Value of startup query interval(in seconds)	IGMP startup query interval in seconds
Value of startup query count	Number of IGMP general queries the device sends on startup
General query timer expiry	Remaining time of the IGMP general query timer
Querier for IGMP	IP address of the IGMP querier
IGMP activity	IGMP activity statistics (joins and leaves)
Robustness	IGMP querier's robustness variable, namely the last member query count)
Require-router-alert	Whether to discard IGMP messages without the Router-Alert option
Fast-leave	Fast leave processing status
Startup-query-timer-expiry	Remaining time of the startup query timer
Other-querier-present-timer-expiry	Remaining time of the other querier present timer
Total 1 IGMP Group reported	Total number of reported groups on the interface

display igmp routing-table

Syntax **display igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*source-address* [**mask** { *mask* | *mask-length* }] | *group-address* [**mask** { *mask* | *mask-length* }]] *

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Multicast source address.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast source address, this argument has an effective value range of 0 to 32; for a multicast group address, this argument has an effective value range of 4 to 32. The system default is 32 in both cases.

Description Use the **display igmp routing-table** command to view the IGMP routing table information.

Example # View IGMP routing table information in the public instance.

```
<Sysname> display igmp routing-table
Routing table of VPN-Instance: public net
 Total 2 entries

 00001. (*, 225.1.1.1)
       List of 1 downstream interface
        Ethernet1/0 (20.1.1.1),
                   Protocol: STATIC

 00002. (*, 239.255.255.250)
       List of 1 downstream interface
        Ethernet1/0 (20.20.20.20),
                   Protocol: IGMP
```

Table 330 Description on the fields of the display igmp routing-table command

Field	Description
00001	Sequence number the (*, G) entry
(*, 225.1.1.1)	A (*, G) entry of the IGMP routing table
List of 1 downstream interface	Downstream interface list: these interfaces need to forward multicast packets

fast-leave (IGMP view)

Syntax **fast-leave** [**group-policy** *acl-number*]

undo fast-leave

View Public instance IGMP view, VPN instance IGMP view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999.

Description Use the **fast-leave** command to enable the fast-leave function for multicast group members globally.

Use the **undo fast-leave** command to disable the fast-leave function globally.

By default, the fast-leave function is disabled, namely, the IGMP querier sends an IGMP group-specific query upon receiving an IGMP leave message from a host, instead of sending a Leave notification directly to the upstream.

Related command: **igmp fast-leave**, **last-member-query-interval**.

This command takes effect on all Layer 3 interfaces when executed in IGMP view.

Example # Enable the fast leave function globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] fast-leave
```

igmp

Syntax **igmp** [**vpn-instance** *vpn-instance-name*]

undo igmp [**vpn-instance** *vpn-instance-name*]

View System view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

Description Use the **igmp** command to enter public instance IGMP view or VPN instance IGMP view.

Use the **undo igmp** command to remove configurations performed in public instance IGMP view or VPN instance IGMP view.

IP multicast must be enabled on the device in the corresponding instance before this command can take effect.

Related command: **igmp enable**, and **multicast routing-enable** on page 1341.

Example # Enable IP multicast routing in the public instance and enter public instance IGMP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] igmp
[Sysname-igmp]
```

Enable IP multicast routing in VPN instance mvpn and enter IGMP view for VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] igmp vpn-instance mvpn
[Sysname-igmp-mvpn]
```

igmp enable

Syntax **igmp enable**

undo igmp enable

View Interface view

Parameter None

Description Use the **igmp enable** command to enable IGMP on the current interface.

Use the **undo igmp enable** command to disable IGMP on the current interface.

By default, IGMP is disabled on all interfaces.

Note that:

- IP multicast must be enabled on the device before this command can take effect.
- IGMP must be enabled on an interface before any other IGMP feature configured on the interface can take effect.

Related command: **igmp**.

Example # Enable IGMP on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp enable
```

igmp fast-leave

Syntax **igmp fast-leave** [**group-policy** *acl-number*]

undo igmp fast-leave

View Interface view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, this command will take effect for all multicast groups.

Description Use the **igmp fast-leave** command to enable the fast leave function on the current interface for multicast group members.

Use the **undo igmp fast-leave** command to disable the fast leave function on the current interface.

By default, the fast leave function is disabled, namely, the IGMP querier sends an IGMP group-specific query upon receiving an IGMP leave message from a host, instead of sending a Leave notification directly to the upstream.

Related command: **fast-leave (IGMP view)** and **igmp last-member-query-interval**.

Example # Enable fast leave for multicast group members on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp fast-leave
```

igmp group-policy

Syntax **igmp group-policy** *acl-number* [*version-number*]

undo igmp group-policy

View Interface view

Parameter *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999.

version-number: IGMP version, in the range of 1 to 3. If you do not specify an IGMP version, the configured group filter will apply to IGMP reports of all versions.

Description Use the **igmp group-policy** command to configure a multicast group filter on the current interface to control joins to specific multicast groups.

Use the **undo igmp group-policy** command to remove the configured multicast group filter.

By default, no multicast group filter is configured, namely a host can join any multicast group.

When you use an advanced ACL as a filter, the source address in the ACL rule is the address of the multicast source specified in the IGMPv3 reports, rather than the source address in the IP packets.

Example # Configure an ACL rule so that hosts on the subnet attached to Ethernet 1/0 can join multicast group 225.1.1.1 only.

```
<Sysname> system-view
[Sysname] acl number 2005
[Sysname-acl-basic-2005] rule permit source 225.1.1.1 0
[Sysname-acl-basic-2005] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp group-policy 2005
```

igmp last-member-query-interval

Syntax **igmp last-member-query-interval** *interval*

undo igmp last-member-query-interval

View Interface view

Parameter *interval*: IGMP last-member query interval in seconds, with an effective range of 1 to 5.

Description Use the **igmp last-member-query-interval** command to configure the last-member query interval on the current interface.

Use the **undo igmp last-member-query-interval** command to restore the last member query interval to the system default on the current interface.

By default, the last-member query interval is 1 second.

Related commands: **last-member-query-interval**, **igmp robust-count**, **display igmp interface**.

Example # Set the last member query interval to 3 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp last-member-query-interval 3
```

igmp max-response-time

Syntax **igmp max-response-time** *interval*

undo igmp max-response-time

View Interface view

Parameter *interval*: Maximum response time in seconds for IGMP general queries, with an effective range of 1 to 25.

Description Use the **igmp max-response-time** command to configure the maximum response time for IGMP general queries on the current interface.

Use the **undo igmp max-response-time** command to restore the maximum response time for IGMP general queries to the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related command: **max-response-time (IGMP view)**, **igmp timer other-querier-present**, **display igmp interface**.

Example # Set the maximum response time for IGMP general queries to 8 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp max-response-time 8
```

igmp require-router-alert

Syntax **igmp require-router-alert**

undo igmp require-router-alert

View Interface view

Parameter None

Description Use the **igmp require-router-alert** command to configure the interface to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo igmp require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, namely it passes all the IGMP messages it receives to the upper layer protocol for processing.

Related command: **require-router-alert (IGMP view)**, **igmp send-router-alert**.

Example # Configure Ethernet 1/0 to discard IGMP messages that do not carry the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp require-router-alert
```

igmp robust-count

Syntax **igmp robust-count** *robust-value*

undo igmp robust-count

View Interface view

Parameter *robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

Description Use the **igmp robust-count** command to configure the IGMP robustness variable on the current interface.

Use the **undo igmp robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related command: **robust-count (IGMP view)**, **igmp timer query**, **igmp last-member-query-interval**, **igmp timer other-querier-present**, **display igmp interface**.

Example # Set the IGMP querier robustness variable to 3 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp robust-count 3
```

igmp send-router-alert

Syntax **igmp send-router-alert**

undo igmp send-router-alert

View Interface view

Parameter None

Description Use the **igmp send-router-alert** command on the current interface to enable insertion of the Router-Alert option in IGMP messages to be sent.

Use the **undo igmp send-router-alert** command on the current interface to disable insertion of the Router-Alert option in IGMP messages to be sent.

By default, IGMP messages are sent with the Router-Alert option.

Related command: **send-router-alert (IGMP view)**, **igmp require-router-alert**.

Example # Disable insertion of the Router-Alert option into IGMP messages that leave Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo igmp send-router-alert
```

igmp static-group

Syntax **igmp static-group** *group-address* [**source** *source-address*]

undo igmp static-group { **all** | *group-address* [**source** *source-address*] }

View Interface view

Parameter **all**: Specifies to remove all static multicast groups that the current interface has joined.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address.

Description Use the **igmp static-group** command to configure the current interface to be a statically connected member of the specified multicast group.

Use the **undo igmp static-group** command to remove the current interface as a statically connected member of the specified multicast group.

By default, an interface is not a static member of any multicast group.

If the specified multicast address is in the SSM multicast address range, and if a multicast source address is specified in the command, multicasts carrying the (S, G) entry, namely the source address information, can be sent out through this interface.

Example # Configure Ethernet 1/0 to be a statically connected member of multicast group 224.1.1.1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp static-group 224.1.1.1
```

Configure Ethernet 1/0 so that it can forward multicasts that multicast source 192.168.1.1 sends to multicast group 232.1.1.1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp static-group 232.1.1.1 source 192.168.1.1
```

igmp timer other-querier-present

Syntax **igmp timer other-querier-present** *interval*

undo igmp timer other-querier-present

View Interface view

Parameter *interval*: IGMP other querier present interval in seconds, in the range of 60 to 300.

Description Use the **igmp timer other-querier-present** command to configure the IGMP other querier present interval on the current interface.

Use the **undo igmp timer other-querier-present** command to restore the system default configuration.

By default, the IGMP other querier present interval is [IGMP query interval] times [IGMP querier robustness variable] plus [maximum response time for IGMP general queries] divided by two.

The three parameters in the above-mentioned formula default to 60 (seconds), 2 (times) and 10 (seconds) respectively, so the default other querier present interval = 60 × 2 + 10 / 2 = 125 (seconds).

Related command: **timer other-querier-present (IGMP view)**, **igmp timer query**, **igmp robust-count**, **igmp max-response-time**, **display igmp interface**.

Example # Set the other querier present interval to 200 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp timer other-querier-present 200
```

igmp timer query

Syntax **igmp timer query** *interval*

undo igmp timer query

View Interface view

Parameter *interval*: IGMP query interval in seconds, namely the interval between IGMP general queries sent by the querier, with an effective range of 1 to 18,000.

Description Use the **igmp timer query** command to configure the IGMP query interval on the current interface.

Use the **undo igmp timer query** command to restore the system default.

By default, the IGMP query interval is 60 seconds.

Related command: **timer query (IGMP view)**, **igmp timer other-querier-present**, **display igmp interface**.

Example # Set the IGMP general query interval to 125 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp timer query 125
```

igmp version

Syntax **igmp version** *version-number*

undo igmp version

View Interface view

Parameter *version-number*: IGMP version, in the range of 1 to 3.

Description Use the **igmp version** command to configure the IGMP version on the current interface.

Use the **undo igmp version** command to restore the IGMP version to the system default.

The default IGMP version is version 2.

Related command: **version (IGMP view)**.

Example # Set the IGMP version to IGMPv1 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] igmp version 1
```

last-member-query-interval

Syntax **last-member-query-interval** *interval*

undo last-member-query-interval

View Public instance IGMP view, VPN instance IGMP view

Parameter *interval*: Last-member query interval, namely the interval in seconds at which the IGMP querier sends IGMP group-specific queries after it receives a leave-group message from a host, with an effective range of 1 to 5.

Description Use the **last-member-query-interval** command to configure the global IGMP last-member query interval.

Use the **undo last-member-query-interval** command to restore the global IGMP last member query interval to the system default.

By default, the IGMP last-member query interval is 1 second.

Related command: **igmp last-member-query-interval**, **robust-count (IGMP view)**, **display igmp interface**.

Example # Set the global IGMP last-member interval to 3 seconds in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] last-member-query-interval 3
```

max-response-time (IGMP view)

Syntax **max-response-time** *interval*

undo igmp max-response-time

View Public instance IGMP view, VPN instance IGMP view

Parameter *interval*: Maximum response time for IGMP general queries in seconds, with an effective range of 1 to 25.

Description Use the **max-response-time** command to configure the maximum response time for IGMP general queries.

Use the **undo max-response-time** command to restore globally the maximum response time for IGMP general queries to the system default.

By default, the maximum response time for IGMP general queries is 10 seconds.

Related command: **igmp max-response-time**, **timer other-querier-present (IGMP view)**, **display igmp interface**.

Example # Set the maximum response time for IGMP general queries to 8 seconds globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] max-response-time 8
```

require-router-alert (IGMP view)

Syntax **require-router-alert**

undo require-router-alert

View Public instance IGMP view, VPN instance IGMP view

Parameter None

Description Use the **require-router-alert** command to configure globally the router to discard IGMP messages that do not carry the Router-Alert option.

Use the **undo require-router-alert** command to restore the system default.

By default, the device does not check the Router-Alert option, namely it handles all the IGMP messages it received to the upper layer protocol for processing.

Related command: **igmp require-router-alert**, **send-router-alert (IGMP view)**.

Example # Globally configure the router to discard IGMP messages that do not carry the Router-Alert option in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] require-router-alert
```

reset igmp group

Syntax **reset igmp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **group** { **all** | **interface** *interface-type interface-number* { **all** | *group-address* [**mask** { *mask* | *mask-length* }] [*source-address* [**mask** { *mask* | *mask-length* }]] } }

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

all: Specifies to clear all IGMP forwarding entries.

interface *interface-type interface-number*: Clears the IGMP forwarding entries on the specified interface.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address.

mask: Subnet mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Subnet mask length of the multicast group/source address. For a multicast group address, this argument has an effective value range of 4 to 32; for

a multicast source address, this argument has an effective value range of 0 to 32. The system default is 32 in both cases.

Description Use the **reset igmp group** command to clear IGMP forwarding entries.

Note that:

- When clearing the IGMP forwarding entries of a VLAN interface, this command also clears the IGMP Snooping forwarding entries for that VLAN.
- This command cannot clear IGMP forwarding entries of static joins.

Related command: **display igmp group**.

Example # Clear all the IGMP forwarding entries on all interfaces in the public instance.

```
<Sysname> reset igmp group all
```

Clear all the IGMP forwarding entries on Ethernet 1/0 in the public instance.

```
<Sysname> reset igmp group interface ethernet 1/0 all
```

Clear the IGMP forwarding entries for multicast group 225.0.0.1 on Ethernet 1/0 in the public instance.

```
<Sysname> reset igmp group interface ethernet 1/0 225.0.0.1
```

Clear the IGMP forwarding entries for multicast groups in the 225.1.1.0/24 segment on Ethernet 1/0 in the public instance.

```
<Sysname> reset igmp group interface ethernet 1/0 225.1.1.0 mask 24
```

robust-count (IGMP view)

Syntax **robust-count** *robust-value*

undo robust-count

View Public instance IGMP view, VPN instance IGMP view

Parameter *robust-value*: IGMP querier robustness variable, with an effective range of 2 to 5. The IGMP robustness variable determines the number of general queries the IGMP querier sends on startup and the number of IGMP group-specific queries the IGMP querier sends upon receiving an IGMP leave message.

Description Use the **robust-count** command to configure the IGMP querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the IGMP querier robustness variable is 2.

Related command: **igmp robust-count**, **timer query (IGMP view)**, **last-member-query-interval**, **timer other-querier-present (IGMP view)**, **display igmp interface**.

Example # Set the IGMP querier robustness variable to 3 globally in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] robust-count 3
```

send-router-alert (IGMP view)

Syntax **send-router-alert**

undo send-router-alert

View Public instance IGMP view, VPN instance IGMP view

Parameter None

Description Use the **send-router-alert** command to globally enable the insertion of the Router-Alert option into IGMP messages to be sent.

Use the **undo send-router-alert** command to globally disable the insertion of the Router-Alert option into IGMP messages to be sent.

By default, an IGMP message carries the Router-Alert option.

Related command: **igmp send-router-alert**, **require-router-alert (IGMP view)**.

Example # Globally disable the insertion of the Router-Alert option in IGMP messages to be sent in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] send-router-alert
```

timer other-querier-present (IGMP view)

Syntax **timer other-querier-present** *interval*

undo timer other-querier-present

View Public instance IGMP view, VPN instance IGMP view

Parameters *interval*: IGMP other querier present interval, in the range of 60 to 300.

Description Use the **timer other-querier-present** command to configure the IGMP other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the system default.

By default, the IGMP other querier present interval is [IGMP query interval] times [IGMP querier robustness variable] plus [maximum response time for IGMP general queries] divided by two.

The three parameters in the above-mentioned formula default to 60 (seconds), 2 (times) and 10 (seconds) respectively, so the default other querier present interval = 60 × 2 + 10 / 2 = 125 (seconds).

Related command: **igmp timer other-querier-present**, **timer query (IGMP view)**, **robust-count (IGMP view)**, **max-response-time (IGMP view)**, **display igmp interface**.

Example # Set the global value of the other querier present interval to 200 seconds in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer other-querier-present 200
```

timer query (IGMP view)

Syntax **timer query** *interval*

undo timer query

View Public instance IGMP view, VPN instance IGMP view

Parameter *interval*: IGMP query interval in seconds, namely interval between IGMP general queries sent by the querier, with an effective range of 1 to 18,000.

Description Use the **timer query** command to configure the IGMP query interval globally.

Use the **undo timer query** command to restore the default setting.

By default, IGMP query interval is 60 seconds.

Related commands: **igmp timer query**, **timer other-querier-present (IGMP view)**, **display igmp interface**.

Example # Set the global value of the IGMP query interval to 125 seconds in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] timer query 125
```

version (IGMP view)

Syntax **version** *version-number*

undo version

View Public instance IGMP view, VPN instance IGMP view

Parameter *version-number*: IGMP version, in the range of 1 to 3.

Description Use the **version** command to configure the global IGMP version.

Use the **undo version** command to restore the global IGMP version to the system default.

The default IGMP version is version 2.

Related command: **igmp version**.

Example # Set the global IGMP version to IGMPv1 in the public instance.

```
<Sysname> system-view
[Sysname] igmp
[Sysname-igmp] version 1
```

89 MSDP CONFIGURATION COMMANDS

cache-sa-enable

Syntax **cache-sa-enable**

undo cache-sa-enable

View Public instance MSDP view, VPN instance MSDP view

Parameter None

Description Use the **cache-sa-enable** command to enable the SA message cache mechanism.

Use the **undo cache-sa-enable** command to disable the SA message cache mechanism.

By default, the SA message cache mechanism is enabled.

Example # Enable the SA message cache mechanism in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] cache-sa-enable
```

display msdp brief

Syntax **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **brief** [**state** { **connect** | **down** | **listen** | **shutdown** | **up** }]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

state: Displays the information of MSDP peers in the specified state.

connect: Displays the information of MSDP peers in the connecting state.

down: Displays the information of MSDP peers in the down state.

listen: Displays the information of MSDP peers in the listening state.

shutdown: Displays the information of MSDP peers in the deactivated state.

up: Displays the information of MSDP peers in the in-session state.

Description Use the **display msdp brief** command to view the brief information of MSDP peers.

Example # View the brief information of MSDP peers in all states in the public instance.

```
<Sysname> display msdp brief
MSDP Peer Brief Information of VPN-Instance: public net
  Configured   Up           Listen       Connect      Shutdown     Down
  1            1            0            0            0            0

  Peer's Address    State    Up/Down time    AS     SA Count   Reset Count
    20.20.20.20       Up       00:00:13        100    0          0
```

Table 331 Description on the fields of the display msdp brief command

Field	Description
Peer's Address	MSDP peer address
State	MSDP peer status: ■ Up: Session set up; MSDP peer in session ■ Listen: Session set up; local device as server, in listening state ■ Connect: Session not set up; local device as client, in connecting state ■ Shutdown: Deactivated ■ Down: Connection failed
Up/Down time	Length of time since MSDP peer connection was established/failed
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
SA Count	Number of (S, G) entries
Reset Count	MSDP peer connection reset times

display msdp peer-status

Syntax **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer-status** [*peer-address*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

peer-address: Specifies an MSDP peer to view the detailed status information about. If you do not provide this argument, this command will display the detailed status information of all MSDP peers.

Description Use the **display msdp peer-status** command to view the detailed MSDP peer status information.

Related command: **peer connect-interface**, **peer description**, **peer mesh-group**, **peer minimum-ttl**, **peer request-sa-enable**, **peer sa-cache-maximum**, **peer sa-policy**, and **peer sa-request-policy**.

Example # View the detailed status information of the MSDP peer with the address of 10.110.11.11 in the public instance.

```
<Sysname> display msdp peer-status 10.110.11.11
MSDP Peer Information of VPN-Instance: public net
  MSDP Peer 20.20.20.20, AS 100
  Description:
  Information about connection status:
    State: Up
    Up/down time: 14:41:08
    Resets: 0
    Connection interface: LoopBack0 (20.20.20.30)
    Number of sent/received messages: 867/947
    Number of discarded output messages: 0
    Elapsed time since last connection or counters clear: 14:42:40
  Information about (Source, Group)-based SA filtering policy:
    Import policy: none
    Export policy: none
  Information about SA-Requests:
    Policy to accept SA-Request messages: none
    Sending SA-Requests status: disable
  Minimum TTL to forward SA with encapsulated data: 0
  SAs learned from this peer: 0, SA-cache maximum for the peer: none
  Input queue size: 0, Output queue size: 0
  Counters for MSDP message:
    Count of RPF check failure: 0
    Incoming/outgoing SA messages: 0/0
    Incoming/outgoing SA requests: 0/0
    Incoming/outgoing SA responses: 0/0
    Incoming/outgoing data packets: 0/0
```

Table 332 Description on the fields of the display msdp peer-status command

Field	Description
MSDP Peer	MSDP peer address
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
State	MSDP peer status: ■ Up: Session set up; MSDP peer in session ■ Listen: Session set up; local device as server, in listening state ■ Connect: Session not set up; local device as client, in connecting state ■ Shutdown: Deactivated ■ Down: Connection failed
Resets	Number of times the MSDP peer connection is reset
Up/Down time	Length of time since MSDP peer connection was established/failed

Table 332 Description on the fields of the display msdp peer-status command

Field	Description
Connection interface	Interface and its IP address used for setting up a TCP connection with the remote MSDP peer
Number of sent/received messages	Number of SA messages sent and received through this connection
Number of discarded output messages	Number of discarded outgoing messages
Elapsed time since last connection or counters clear	Time passed since the information of the MSDP peer was last cleared
Information about (Source, Group)-based SA filtering policy	SA message filtering list information ■ Import policy: Filter list for receiving SA messages from the specified MSDP peer ■ Export policy: Filter list for forwarding SA messages from the specified MSDP peer
Information about SA-Requests	SA requests information ■ Policy to accept SA-Request messages: Filtering rule for receiving or forwarding SA messages from the specified MSDP peer ■ Sending SA-Requests status: Whether enabled to send an SA request message to the designated MSDP peer upon receiving a new Join message
Minimum TTL to forward SA with encapsulated data	Minimum TTL of multicast packet encapsulated in SA messages
SAs learned from this peer	Number of cached SA messages
SA-cache maximum for the peer	Maximum number of SA messages from the specified MSDP peer that can be cached
Input queue size	Data size cached in the input queue
Output queue size	Data size cached in the output queue
Counters for MSDP message	MSDP peer statistics: ■ Count of RPF check failure: Number of SA messages discarded due to RPF check failure ■ Incoming/outgoing SA messages: Number of SA messages received and sent ■ Incoming/outgoing SA requests: Number of SA request received and sent ■ Incoming/outgoing SA responses: Number of SA responses received and sent ■ Incoming/outgoing data packets: Number of received and sent SA messages encapsulated with multicast data

display msdp sa-cache

Syntax **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address* | *source-address* | *as-number*] *

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Multicast group address in the (S, G) entry, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Multicast source address in the (S, G) entry.

as-number: AS number, in the range of 1 to 65535.

Description Use the **display msdp sa-cache** command to view the information of (S, G) entries in the MSDP cache.

Note that:

- This command gives the corresponding output only after the **cache-sa-enable** command is executed.
- If you do not provide a source address, this command will display the information of all sources in the specified multicast group.
- If you do not provide a group address and a source address, this command will display the information of all cached entries.
- If you do not provide an AS number, this command will display the information related to all ASs.

Related command: **cache-sa-enable**.

Example # View the information of (S, G) entries in the MSDP cache in the public instance.

```
<Sysname> display msdp sa-cache
MSDP Source-Active Cache Information of VPN-Instance: public net
 MSDP Total Source-Active Cache - 5 entries
 MSDP matched 5 entries

 (Source, Group)                Origin RP      Pro  AS    Uptime   Expires
 (10.10.1.2, 225.1.1.1)           10.10.10.10     BGP  100   00:00:10 00:05:50
 (10.10.1.3, 225.1.1.1)           10.10.10.10     BGP  100   00:00:11 00:05:49
 (10.10.1.2, 225.1.1.2)           10.10.10.10     BGP  100   00:00:11 00:05:49
 (10.10.2.1, 225.1.1.2)           10.10.10.10     BGP  100   00:00:11 00:05:49
 (10.10.1.2, 225.1.2.2)           10.10.10.10     BGP  100   00:00:11 00:05:49
```

Table 333 Description on the fields of the display msdp sa-cache command

Field	Description
(Source, Group)	(S, G) entry: (source address, group address)
Origin RP	Address of the RP that generated the (S, G) entry
Pro	Type of protocol from which the AS number is originated. "?" indicates that the system was unable to obtain the protocol type.
AS	AS number of the origin RP. "?" indicates that the system was unable to obtain the AS number.
Uptime	Length of time for which the cached (S, G) entry has been existing, in hours:minutes:seconds
Expires	Length of time in which the cached (S, G) entry will expire, in hours:minutes:seconds

display msdp sa-count

Syntax **display msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-count** [*as-number*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

as-number: AS number, in the range of 1 to 65535.

Description Use the **display msdp sa-count** command to view the number of SA messages in the MSDP cache.

This command gives the corresponding output only after the **cache-sa-enable** command is executed.

Related command: **cache-sa-enable**.

Example # View the number of SA messages in the MSDP cache in the public instance.

```
<Sysname> display msdp sa-count
MSDP Source-Active Count Information of VPN-Instance: public net
  Number of cached Source-Active entries, counted by Peer
  Peer's Address     Number of SA
  10.10.10.10        5

  Number of source and group, counted by AS
  AS     Number of source    Number of group
  ?      3                   3

  Total 5 Source-Active entries
```

Table 334 Description on the fields of the display msdp sa-count command

Field	Description
Number of cached Source-Active entries, counted by Peer	Number of SA messages counted by peer
Peer's Address	MSDP peer addresses
Number of SA	Number of SA messages from this peer
AS	Number of the AS where the MSDP peer is located. "?" indicates that the system was unable to obtain the AS number.
Number of source	Number of multicast sources from this AS
Number of group	Number of multicast groups from this AS

encap-data-enable

Syntax **encap-data-enable**

undo encap-data-enable

View Public instance MSDP view, VPN instance MSDP view

Parameter None

Description Use the **encap-data-enable** command to enable register message encapsulation in SA messages.

Use the **undo encap-data-enable** command to disable register message encapsulation in SA messages.

By default, an SA message contains only an (S, G) entry. No register message is encapsulated in an SA message.

Example # Enable register message encapsulation in SA messages in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] encap-data-enable
```

import-source

Syntax **import-source** [**acl** *acl-number*]

undo import-source

View Public instance MSDP view, VPN instance MSDP view

Parameter *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999. A basic ACL is used to filter the multicast sources; while an advanced ACL is used to filter the multicast sources or multicast groups. If you do not provide this argument in your command, no multicast source information will be advertised.

During ACL matching, the protocol ID in the ACL rule is not checked.

Description Use the **import-source** command to configure a rule of creating (S, G) entries.

Use the **undo import-source** command to remove any rule of creating (S, G) entries.

By default, when an SA message is created, there are no restrictions on the (S, G) entries to be advertised in it, namely all the (S, G) entries within the domain are advertised in the SA message.

In addition to controlling SA message creation by using this command, you can also configure a filtering rule for forwarding and receiving SA messages by using the **peer sa-policy** command.

Related command: **peer sa-policy**.

Example # Configure the MSDP peer in the public instance to advertise only the (S, G) entries of multicast sources on the 10.10.0.0/16 subnet and with multicast group address of 225.1.0.0/16 when creating an SA message.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit ip source 10.10.0.0 0.0.255.255 d
estination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3101] quit
[Sysname] msdp
[Sysname-msdp] import-source acl 3101
```

msdp

Syntax **msdp** [**vpn-instance** *vpn-instance-name*]

undo msdp [**vpn-instance** *vpn-instance-name*]

View System view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

Description Use the **msdp** command to enable MSDP in the public instance or the specified VPN instance and enter public instance or VPN instance MSDP view.

Use the **undo msdp** command to disable MSDP in the public instance or the specified VPN instance and remove the configurations performed in public instance or VPN instance MSDP view to free the resources occupied by MSDP.

By default, MSDP is disabled.

IP multicast must be enabled in the corresponding instance on the device before this command is meaningful.

Related command: **display multicast routing-table** on page 1331.

Example # Enable IP multicast routing in the public instance, and enable MSDP in the public instance and enter public instance MSDP view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] msdp
[Sysname-msdp]
```

Enable IP multicast routing in VPN instance mvpn, and enable MSDP in VPN instance mvpn and enter MSDP view of VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn]route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] msdp vpn-instance mvpn
[Sysname-msdp-mvpn]
```

originating-rp

Syntax **originating-rp** *interface-type interface-number*

undo originating-rp

View Public instance MSDP view, VPN instance MSDP view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **originating-rp** command to configure the address of the specified interface as the RP address of SA messages.

Use the **undo originating-rp** command to restore the system default.

Be default, the PIM RP address is used as the RP address of SA messages.

Example # Specify the IP address of Ethernet 1/0 as the RP address of SA messages in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] originating-rp ethernet 1/0
```

peer connect-interface

Syntax **peer** *peer-address* **connect-interface** *interface-type interface-number*

undo peer *peer-address*

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

interface-type interface-number: Specifies an interface by its type and number. The local device will use the IP address of the specified interface as the source IP address when setting up a TCP connection with the remote MSDP peer.

Description Use the **peer connect-interface** command to create an MSDP peer connection.

Use the **undo peer connect-interface** command to remove an MSDP peer connection.

No MSDP peer connection is created by default.

Be sure to carry out this command before you use any other **peer** command; otherwise the system will prompt that the peer does not exist.

Related command: **static-rpf-peer**.

Example # Configure the router with the IP address of 125.10.7.6 in the public instance as the MSDP peer of the local router, with interface Ethernet 1/0 as the local connection port.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface ethernet 1/0
```

peer description

Syntax **peer** *peer-address* **description** *text*

undo peer *peer-address* **description**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

text: Descriptive text, a string of 1 to 80 characters (case sensitive).

Description Use the **peer description** command to configure the description information for the specified MSDP peer.

Use the **undo peer description** command to delete the configured description information of the specified MSDP peer.

By default, an MSDP peer has no description information.

Related command: **display msdp peer-status**.

Example # In the public instance, add the descriptive text "Router CstmrA" for the router with the IP address of 125.10.7.6 to indicate that this router is Customer A.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 description Router CstmrA
```

peer mesh-group

Syntax **peer** *peer-address* **mesh-group** *name*

undo peer *peer-address* **mesh-group**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

name: Mesh group name, a string of 1 to 32 characters (case sensitive).

Description Use the **peer mesh-group** command to configure an MSDP peer as a mesh group member.

Use the **undo peer mesh-group** command to remove an MSDP peer as a mesh group member.

By default, an MSDP peer does not belong to any mesh group.

Example # In the public instance, configure the MSDP peer with the IP address of 125.10.7.6 as a member of the mesh group "Grp1".

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 mesh-group Grp1
```

peer minimum-ttl

Syntax **peer** *peer-address* **minimum-ttl** *ttl-value*

undo peer *peer-address* **minimum-ttl**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

ttl-value: Time to live (TTL) value, in the range of 0 to 255.

Description Use the **peer minimum-ttl** command to configure the minimum TTL value of multicast packets encapsulated in SA messages.

Use the **undo peer minimum-ttl** command to restore the default setting.

By default, the minimum TTL value of a multicast packet encapsulated in an SA message is 0.

Related command: **display msdp peer-status**.

Example # In the public instance, set the minimum TTL value of multicast packets to be encapsulated in SA messages to 10 so that only multicast packets whose TTL value is larger than or equal to 10 can be forwarded to the MSDP peer 110.10.10.1.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 110.10.10.1 minimum-ttl 10
```

peer request-sa-enable

Syntax **peer** *peer-address* **request-sa-enable**

undo peer *peer-address* **request-sa-enable**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

Description Use the **peer request-sa-enable** command to enable the device to send SA request messages.

Use the **undo peer request-sa-enable** command to disable the device from sending SA request messages.

By default, no SA request message is sent.

Note that before you can enable the device to send SA requests, you must disable the SA message cache mechanism.

Related command: **cache-sa-enable**.

Example # Disable the SA message cache mechanism in the public instance, and enable the router to send an SA request message to the MSDP peer 125.10.7.6 upon receiving a new Join message..

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] undo cache-sa-enable
[Sysname-msdp] peer 125.10.7.6 request-sa-enable
```

peer sa-cache-maximum

Syntax **peer** *peer-address* **sa-cache-maximum** *sa-limit*

undo peer *peer-address* **sa-cache-maximum**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

sa-limit: Maximum number of SA messages that the device can cache, in the range of 1 to 8,192.

Description Use the **peer sa-cache-maximum** command to configure the maximum number of SA messages that the device can cache.

Use the **undo peer sa-cache-maximum** command to restore the default setting.

By default, the device can cache a maximum of 8,192 SA messages.

Related command: **display msdp sa-count**, **display msdp peer-status**, and **display msdp brief**.

Example # In the public instance allow the device to cache a maximum of 100 SA messages from the MSDP peer 125.10.7.6.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 sa-cache-maximum 100
```

peer sa-policy

Syntax **peer** *peer-address* **sa-policy** { **import** | **export** } [**acl** *acl-number*]

undo peer *peer-address* **sa-policy** { **import** | **export** }

View Public instance MSDP view, VPN instance MSDP view

Parameter **import**: Specifies to filter SA messages from the specified MSDP peer.

export: Specifies to filter SA messages forwarded to the specified MSDP peer.

peer-address: MSDP peer address.

acl-number: Advanced ACL number, in the range of 3000 to 3999. If you do not provide an ACL number, all SA messages carrying (S, G) entries will be filtered off.

Description Use the **peer sa-policy** command to configure a filtering rule for receiving or forwarding SA messages.

Use the **undo peer sa-policy** command to restore the default setting.

By default, SA messages received or to be forwarded are not filtered, namely, all SA messages are accepted or forwarded.

In addition to controlling SA message receiving and forwarding by using this command, you can also configure a filtering rule for creating SA messages using the **import-source** command.

Related command: **display msdp peer-status** and **import-source**.

Example # Configure a filtering rule in the public instance so that SA messages will be forwarded to MSDP peer 125.10.7.6 only if they match ACL 3100.

```
<Sysname> system-view
[Sysname] acl number 3100
[Sysname-acl-adv-3100] rule permit ip source 170.15.0.0 0.0.255.255
destination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3100] quit
[Sysname] msdp
[Sysname-msdp] peer 125.10.7.6 connect-interface ethernet 1/0
[Sysname-msdp] peer 125.10.7.6 sa-policy export acl 3100
```

peer sa-request-policy

Syntax **peer** *peer-address* **sa-request-policy** [**acl** *acl-number*]

undo peer *peer-address* **sa-request-policy**

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

acl-number: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the SA requests of only the multicast groups that match the ACL will be accepted and other SA requests will be ignored; if you do not provide this argument, all SA requests will be ignored.

Description Use the **peer sa-request-policy** command to configure a filtering rule for SA request messages.

Use the **undo peer sa-request-policy** command to remove the configured SA request filtering rule.

Be default, SA request messages are not filtered.

Related command: **display msdp peer-status**.

Example # Configure an SA request filtering rule in the public instance so that SA messages from the MSDP peer 175.58.6.5 will be accepted only if the multicast group address in the SA messages is in the range of 225.1.1.0/24.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 225.1.1.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] msdp
[Sysname-msdp] peer 175.58.6.5 sa-request-policy acl 2001
```

reset msdp peer

Syntax **reset msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **peer** [*peer-address*]

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

peer-address: Address of the MSDP peer with which the TCP connection is to be reset. If you do not provide this argument, the TCP connections with all MSDP peers will be reset.

Description Use the **reset msdp peer** command to reset the TCP connection with the MSDP peer and clear all the statistics information of the MSDP peer

Related command: **display msdp peer-status**.

Example # Reset the TCP connection in the public instance with the MSDP peer 125.10.7.6 and clear all the statistics information of this MSDP peer.

```
<Sysname> reset msdp peer 125.10.7.6
```

reset msdp sa-cache

Syntax **reset msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **sa-cache** [*group-address*]

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Address of the multicast group related to which the (S, G) entries are to be cleared from the MSDP cache. The effective range is 224.0.1.0 to 239.255.255.255. If you do not provide this argument, the command will clear all the cached (S, G) entries.

Description Use the **reset msdp sa-cache** command to clear (S, G) entries from the MSDP cache.

Related command: **cache-sa-enable** and **display msdp sa-cache**.

Example # Clear the (S, G) entries related to the multicast group 225.5.4.3 from the MSDP cache in the public instance.

```
<Sysname> reset msdp sa-cache 225.5.4.3
```

reset msdp statistics

Syntax **reset msdp** [**vpn-instance** *vpn-instance-name* | **all-instance**] **statistics** [*peer-address*]

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

peer-address: Address of the MSDP peer of which the statistics information is to be cleared. If you do not provide this argument, the command will clear the statistics information of all MSDP peers.

Description Use the **reset msdp statistics** command to clear the statistics information of the specified MSDP peer or all MSDP peers without resetting the MSDP peer(s).

Example # Clear the statistics information of the MSDP peer 125.10.7.6 in the public instance.

```
<Sysname> reset msdp statistics 125.10.7.6
```

shutdown (MSDP View)

Syntax **shutdown** *peer-address*

undo shutdown *peer-address*

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

Description Use the **shutdown** command to deactivate manually the connection with the specified MSDP peer.

Use the **undo shutdown** command to reactivate the connection with the specified MSDP peer.

By default, the connections with all MSDP peers are active.

Related command: **display msdp peer-status**.

Example # Deactivate the connection with the MSDP peer 125.10.7.6 in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] shutdown 125.10.7.6
```

static-rpf-peer

Syntax **static-rpf-peer** *peer-address* [**rp-policy** *ip-prefix-name*]

undo static-rpf-peer *peer-address*

View Public instance MSDP view, VPN instance MSDP view

Parameter *peer-address*: MSDP peer address.

rp-policy *ip-prefix-name*: Specifies a filtering policy based on the RP address in SA messages, where *ip-prefix-name* is the filtering policy name, a string of 1 to 19 characters (case sensitive).

Description Use the **static-rpf-peer** command to configure a static RPF peer.

Use the **undo static-rpf-peer** command to remove a static RPF peer.

No static RPF peer is configured by default.

When you configure multiple static RPF peers, observe the follow rules:

1. If you use the **rp-policy** keyword for all the static RPF peers, all the static RPF peers take effect concurrently. SA messages will be filtered as per the configured prefix list and only those SA messages whose RP addresses pass the filtering will be accepted. If multiple static RPF peers use the same filtering policy at the same time, when a peer receives an SA message, it will forward the SA message to the other peers.
2. If you use the **rp-policy** keyword for none of the static RPF peers, according to the configuration sequence, only the first static RPF peer whose connection is in the UP state will be activated, and all SA messages from this peer will be accepted while the SA messages from other static RPF peers will be discarded. When this active static RPF peer fails (for example, when the configuration is removed or when the connection is torn down), still the first RPF peer whose connection is in UP state will be selected as the activated RPF peer according to the configuration sequence.

Related command: **display msdp peer-status** and ip prefix-list.

Example # Configure static RPF peers in the public instance.

```
<Sysname> system-view
[Sysname] ip ip-prefix list1 permit 130.10.0.0 16 great-equal 16 les
s-equal 32
[Sysname] msdp
[Sysname-msdp] peer 130.10.7.6 connect-interface ethernet 1/0
[Sysname-msdp] static-rpf-peer 130.10.7.6 rp-policy list1
```

timer retry

Syntax **timer retry** *interval*

undo timer retry

View Public instance MSDP view, VPN instance MSDP view

Parameter *interval*: Interval between MSDP peer connection retries, in seconds. The effective range is 1 to 60.

Description Use the **timer retry** command to configure the interval between MSDP peer connection retries.

Use the **undo timer retry** command to restore the default setting.

By default, the interval between MSDP peer connection retries is 30 seconds.

Related command: **display msdp peer-status**.

Example # Set the MSDP peer connection retry interval to 60 seconds in the public instance.

```
<Sysname> system-view
[Sysname] msdp
[Sysname-msdp] timer retry 60
```

90 PIM CONFIGURATION COMMANDS

auto-rp enable

Syntax **auto-rp enable**

undo auto-rp enable

View Public instance PIM view, VPN instance PIM view

Parameter None

Description Use the **auto-rp enable** command to enable auto-RP.

Use the **undo auto-rp enable** command to disable auto-RP.

By default, auto-RP is disabled.

Related command: **static-rp (PIM view)**.

Example # Enable auto-RP in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] auto-rp enable
```

bsr-policy (PIM view)

Syntax **bsr-policy** *acl-number*

undo bsr-policy

View Public instance PIM view, VPN instance PIM view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999. When an ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source address range.

Description Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely all the received BSR messages are regarded to be valid.

Example # Configure a legal BSR address range in the public instance so that only routers on the segment 10.1.1.0/24 can become the BSR.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.0 0.0.0.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] bsr-policy 2000
```

c-bsr (PIM view)

Syntax **c-bsr** *interface-type interface-number* [*hash-length* [*priority*]]

undo c-bsr

View Public instance PIM view, VPN instance PIM view

Parameter *interface-type interface-number*: Specifies an interface by its type and number. This configuration can take effect only if PIM-SM is enabled on the interface.

hash-length: Hash mask length for RP selection calculation, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr** command to configure the specified interface as a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Related command: **pim sm**, **c-bsr hash-length (PIM view)**, **c-bsr priority (PIM view)**, and **c-rp (PIM view)**.

Example # Configure Ethernet 1/0 to be a C-BSR in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr ethernet 1/0
```

c-bsr admin-scope

Syntax **c-bsr admin-scope**

undo c-bsr admin-scope

View Public instance PIM view, VPN instance PIM view

Parameter None

Description Use the **c-bsr admin-scope** command to enable BSR administrative scoping to implement RP-Set distribution based on BSR admin-scope regions.

Use the **undo c-bsr admin-scope** command to disable BSR administrative scoping.

By default, BSR administrative scoping is disabled, namely only one BSR exists in each PIM-SM domain.

Related command: **c-bsr (PIM view)**, **c-bsr group**, and **c-bsr global**.

Example # Enable BSR administrative scoping in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr admin-scope
```

c-bsr global

Syntax **c-bsr global** [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr global

View Public instance PIM view, VPN instance PIM view

Parameter *hash-length*: Hash mask length for RP selection calculation in the global scope zone, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the global scope zone, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr global** command to configure a C-BSR for the global scope zone.

Use the **undo c-bsr global** command to remove the C-BSR configuration for the global scope zone.

By default, no C-BSRs are configured for the global scope zone.

Related command: **c-bsr group**, **c-bsr hash-length (PIM view)**, and **c-bsr priority (PIM view)**.

Example # Configure the router to be a C-BSR for the global scope zone in the public instance, with the priority of 1.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr global priority 1
```

c-bsr group

Syntax **c-bsr group** *group-address* { *mask* | *mask-length* } [**hash-length** *hash-length* | **priority** *priority*] *

undo c-bsr group *group-address*

View Public instance PIM view, VPN instance PIM view

Parameter *group-address*: Multicast group address, in the range of 239.0.0.0 to 239.255.255.255.

mask: Mask of the multicast group address.

mask-length: Mask length of the multicast group address, in the range of 8 to 32.

hash-length: Hash mask length for RP selection calculation in the BSR admin-scope region corresponding to the specified multicast group, in the range of 0 to 32. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR in the BSR admin-scope region corresponding to a multicast group, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value of this argument means a higher priority.

Description Use the **c-bsr group** command to configure a C-BSR for the BSR admin-scope region associated with the specified group.

Use the **undo c-bsr group** command to remove the C-BSR configuration for the BSR admin-scope region associated with the specified group.

By default, no C-BSRs are configured for BSR admin-scope regions.

Related command: **c-bsr global**, **c-bsr admin-scope**, **c-bsr hash-length (PIM view)**, and **c-bsr priority (PIM view)**.

Example # In the public instance configure the router to be a C-BSR in the BSR admin-scope region associated with the multicast group address 239.0.0.0/8, with the priority of 10.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr group 239.0.0.0 255.0.0.0 priority 10
```

c-bsr hash-length (PIM view)

Syntax **c-bsr hash-length** *hash-length*

undo c-bsr hash-length

View Public instance PIM view, VPN instance PIM view

Parameter *hash-length*: Hash mask length for RP selection calculation, in the range of 0 to 32.

Description Use the **c-bsr hash-length** command to configure the global Hash mask length for RP selection calculation.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length for RP selection calculation is 30.

Related command: **c-bsr (PIM view)**, **c-bsr global**, and **c-bsr group**.

Example # Set the global Hash mask length for RP selection calculation to 16 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr hash-length 16
```

c-bsr holdtime (PIM view)

Syntax **c-bsr holdtime** *interval*

undo c-bsr holdtime

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Bootstrap timeout in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **c-bsr holdtime** command to configure the bootstrap timeout time, namely the length of time a C-BSR waits before it must receive a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the default setting.

By default, the bootstrap timeout value is determined by this formula: Bootstrap timeout = Bootstrap interval × 2 + 10.

The default bootstrap interval is 60 seconds, so the default bootstrap timeout = 60 × 2 + 10 = 130 (seconds).

Related command: **c-bsr (PIM view)** and **c-bsr interval (PIM view)**.

Example # Set the bootstrap timeout time to 150 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr holdtime 150
```

c-bsr interval (PIM view)

Syntax **c-bsr interval** *interval*

undo c-bsr interval

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Bootstrap interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **c-bsr interval** command to configure the bootstrap interval, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the default setting.

By default, the bootstrap interval value is determined by this formula: Bootstrap interval = (Bootstrap timeout - 10) / 2.

The default bootstrap timeout is 130 seconds, so the default bootstrap interval = (130 - 10) / 2 = 60 (seconds).

Related command: **c-bsr (PIM view)** and **c-bsr holdtime (PIM view)**.

Example # Set the bootstrap interval to 30 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr interval 30
```

c-bsr priority (PIM view)

Syntax **c-bsr priority** *priority*

undo c-bsr priority

View Public instance PIM view, VPN instance PIM view

Parameter *priority*: Priority of the C-BSR, in the range of 0 to 255. A larger value of this argument means a higher priority.

Description Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the default setting.

By default, the C-BSR priority is 0.

Related command: **c-bsr (PIM view)**, **c-bsr global**, and **c-bsr group**.

Example # Set the global C-BSR priority to 5 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-bsr priority 5
```

c-rp (PIM view)

Syntax **c-rp** *interface-type interface-number* [**group-policy** *acl-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *interface-type interface-number*

View Public instance PIM view, VPN instance PIM view

Parameter *interface-type interface-number*: Specifies an interface, the IP address of which will be advertised as a C-RP address.

acl-number: Basic ACL number, in the range of 2000 to 2999. This ACL defines a range of multicast groups the C-RP is going to serve, rather than defining a filtering rule. Any group range matching the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value of this argument means a lower priority.

hold-interval: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not provide this argument in your command, the corresponding global setting will be used.

Description Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- If you do not specify a group range for the C-RP, the C-RP will serve all multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these multiple group ranges in multiple rules in the ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related command: **c-bsr (PIM view)**.

Example # In the public instance configure Ethernet 1/0 to be a C-RP for multicast groups 225.1.0.0/16 and 226.2.0.0/16, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 225.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] rule permit source 226.2.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] c-rp ethernet 1/0 group-policy 2000 priority 10
```

c-rp advertisement-interval (PIM view)

Syntax **c-rp advertisement-interval** *interval*

undo c-rp advertisement-interval

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the default setting.

By default, the C-RP-Adv interval is 60 seconds.

Related command: **c-rp (PIM view)**.

Example # Set the global C-RP-Adv interval to 30 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp advertisement-interval 30
```

c-rp holdtime (PIM view)

Syntax **c-rp holdtime** *interval*

undo c-rp holdtime

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits before it must receive a C-RP-Adv message.

Use the **undo c-rp holdtime** command to restore the default setting.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the bootstrap interval or longer.

Related command: **c-rp (PIM view)** and **c-bsr interval (PIM view)**.

Example # Set the global C-RP timeout time to 200 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] c-rp holdtime 200
```

crp-policy (PIM view)

Syntax **crp-policy** *acl-number*

undo crp-policy

View Public instance PIM view, VPN instance PIM view

Parameter *acl-number*: Advanced ACL number, in the range of 3000 to 3999. When the ACL is defined, the **source** keyword in the **rule** command specifies the address of a C-RP and the **destination** keyword specifies the address range of the multicast groups that the C-RP will serve.

Description Use the **crp-policy** command to configure a legal C-RP address range and the range of served multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are accepted.

Example # In the public instance, configure a C-RP address range and a range of served multicast groups so that only routers in the address range of 1.1.1.1/32 can be C-RPs and these C-RPs can serve only multicast groups in the address range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 1.1.1.1 0 destination 2
25.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] crp-policy 3000
```

display pim bsr-info

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **bsr-info**

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

Description Use the **display pim bsr-info** command to view the BSR information in the PIM domain and the locally configured C-RP information in effect.

Related command: **c-bsr (PIM view)** and **c-rp (PIM view)**.

Example # View the BSR information in the PIM-SM domain in the public instance and the locally configured C-RP information in effect.

```
<Sysname> display pim bsr-info
 Vpn-instance: public net
 Elected BSR Address: 12.12.12.9
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Global
     Uptime: 00:00:56
     Next BSR message scheduled at: 00:01:14
 Candidate BSR Address: 12.12.12.9
     Priority: 0
     Hash mask length: 30
     State: Elected
     Scope: Global
```

```
Candidate RP: 12.12.12.9(LoopBack1)
    Priority: 0
    HoldTime: 150
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
Candidate RP: 3.3.3.3(Ethernet1/0)
    Priority: 20
    HoldTime: 90
    Advertisement Interval: 50
    Next advertisement scheduled at: 00:00:28
Candidate RP: 5.5.5.5(Ethernet1/1)
    Priority: 0
    HoldTime: 80
    Advertisement Interval: 60
    Next advertisement scheduled at: 00:00:48
```

Table 335 Description on the fields of the display pim bsr-info command

Field	Description
Elected BSR Address	Address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length for RP selection calculation
State	BSR state
Scope	Scope of the BSR
Uptime	Length of time for which this BSR has been up, in hours:minutes:seconds
Next BSR message scheduled at	Length of time in which the BSR will expire, in hours:minutes:seconds
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval at which the C-RP sends advertisement messages
Next advertisement scheduled at	Length of time in which the C-RP will send the next advertisement message, in hours:minutes:seconds

display pim claimed-route

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **claimed-route** [*source-address*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

source-address: Displays the information of the unicast route to a particular multicast source. If you do not provide this argument, this command will display the information about all unicast routes used by PIM.

Description Use the **display pim claimed-route** command to view the information of unicast routes used by PIM.

If an (S, G) is marked SPT, this (S, G) entry uses a unicast route.

Example # View the information of all unicast routes used by PIM in the public instance.

```
<Sysname> display pim claimed-route
 Vpn-instance: public net
 RPF information about: 172.168.0.0
     RPF interface: Ethernet1/1, RPF neighbor: 172.168.0.2
     Referenced route/mask: 172.168.0.0/24
     Referenced route type: unicast (direct)
     RPF-route selecting rule: preference-preferred
     The (S,G) or (*,G) list dependent on this route entry
     (172.168.0.12, 227.0.0.1)
```

Table 336 Description on the fields of the display pim claimed-route command

Field	Description
RPF interface	RPF interface type and number
RPF neighbor	IP address of the RPF neighbor
Referenced route/mask	Address/mask of the referenced route
Referenced route type	Type of the referenced route
RPF-route selecting rule	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entries using this route

display pim control-message counters

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graft** | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

probe: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface *interface-type interface-number*: Displays the number of PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of graft messages.

graft-ack: Displays the number of graft-ack messages.

hello: Displays the number of hello messages.

join-prune: Displays the number of join/prune messages.

state-refresh: Displays the number of state refresh messages.

Description Use the **display pim control-message counters** command to view the statistics information of PIM control messages.

Example # View the statistics information of all types of PIM control messages on all interfaces in the public instance.

```
<Sysname> display pim control-message counters
 Vpn-instance: public net
 PIM global control-message counters:
                  Received         Sent             Invalid
 Register         20               37               2
 Register-Stop    25               20               1
 Probe            10               5                0

 PIM control-message counters for interface: Ethernet1/0
                  Received         Sent             Invalid
 Assert           10               5                0
 Graft            20               37               2
 Graft-Ack        25               20               1
 Hello            1232             453              0
 Join/Prune       15               30               21
 State-Refresh    8                7                1
 BSR              3243             589              1
 C-RP             53               32               0
```

Table 337 Description on the fields of display pim control-message counters

Field	Description
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages

Table 337 Description on the fields of display pim control-message counters

Field	Description
C-RP	C-RP-Adv messages

display pim grafts

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **grafts**

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

Description Use the **display pim grafts** command to view the information about unacknowledged graft messages.

Example # View the information about unacknowledged graft messages in the public instance.

```
<Sysname> display pim grafts
 Vpn-instance: public net
 Source             Group             Age           RetransmitIn
 192.168.10.1       224.1.1.1         00:00:24      00:00:02
```

Table 338 Description on the fields of the display pim grafts command

Field	Description
Source	Multicast source address in the graft message
Group	Multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

display pim interface

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

interface-type interface-number: Displays the PIM information on a particular interface.

verbose: Displays the detailed PIM information.

Description Use the **display pim interface** command to view the PIM information on the specified interface or all interfaces.

Example # View the PIM information on all interfaces in the public instance.

```
<Sysname> display pim interface
 Vpn-instance: public net
 Interface           NbrCnt HelloInt   DR-Pri     DR-Address
 Eth1/0              1      30         1          10.1.1.2
 Eth1/1              0      30         1          172.168.0.2     (local)
 Eth1/2              1      30         1          20.1.1.2
```

Table 339 Description on the fields of the display pim interface command

Field	Description
Interface	Interface name
NbrCnt	Number of PIM neighbors
HelloInt	Hello interval
DR-Pri	Priority for DR election
DR-Address	DR IP address

View the detailed PIM information on Ethernet 1/0 in the public instance.

```
<Sysname> display pim interface ethernet 1/0 verbose
 Vpn-instance: public net
 Interface: Ethernet1/0, 10.1.1.1
     PIM version: 2
     PIM mode: Sparse
     PIM DR: 10.1.1.2
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on network not using neighbor tracking: 2
```

Table 340 Description on the fields of the display pim interface verbose command

Field	Description
Interface	Interface name and its IP address
PIM version	Running PIM version
PIM mode	PIM mode, dense or sparse
PIM DR	DR IP address
PIM DR Priority (configured)	Configured priority for DR election
PIM neighbor count	Total number of PIM neighbors
PIM hello interval	Hello interval
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	BSR administrative scoping status (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim join-prune

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *neighbor-address*] * [**verbose**]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

mode: Displays the information of join/prune messages to send in the specified PIM mode. PIM modes include **sm** and **ssm**, which represent PIM-SM and PIM-SSM respectively.

flags *flag-value*: Displays routing entries containing the specified flag. Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

neighbor-address: Displays the information of join/prune messages to send to the specified PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

Description Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Example # View the information of join/prune messages to send in the PIM-SM mode in the public instance.

```
<Sysname> display pim join-prune mode sm
 Vpn-instance: public net

 Expiry Time: 50 sec
 Upstream nbr: 10.1.1.1 (Ethernet1/1)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
 ------------------------------------------------------------------------
 Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 341 Description on the fields of the display pim join-prune command

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IP address of the upstream PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim neighbor

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **neighbor** [**interface** *interface-type interface-number* | *neighbor-address* | **verbose**] *

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

interface-type interface-number: Displays the PIM neighbor information on a particular interface.

neighbor-address: Displays the information of a particular PIM neighbor.

verbose: Displays the detailed PIM neighbor information.

Description Use the **display pim neighbor** command to view the PIM neighbor information.

Example # View the information of all PIM neighbors in the public instance.

```
<Sysname> display pim neighbor
 Vpn-instance: public net
 Total Number of Neighbors = 2

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 10.1.1.2        Eth1/0              02:50:49 00:01:31 1
 20.1.1.2        Eth1/1              02:49:39 00:01:42 1
```

Table 342 Description on the fields of the display pim neighbor command

Field	Description
Total Number of Neighbors	Total number of PIM neighbors
Neighbor	IP address of the PIM neighbor
Interface	Interface connecting the PIM neighbor
Uptime	Length of time for which the PIM neighbor has been up, in hours:minutes:seconds
Expires	Length of time in which the PIM neighbor will expire, in hours:minutes:seconds
Dr-Priority	Designated router priority

View the PIM neighbor information on Ethernet 1/0 of the public instance.

```
<Sysname> display pim neighbor interface ethernet 1/0

 Total Number of Neighbors on this interface  = 3

 Neighbor        Interface           Uptime   Expires  Dr-Priority
 101.110.110.150 Eth1/0              00:37:17 00:01:28 1
 11.110.0.40     Eth1/1              00:33:20 00:01:25 1
 11.110.0.20     Eth1/2              00:04:53 00:01:22 1
```

View the detailed information of the PIM neighbor whose IP address is 11.110.0.20.

```
<Sysname> display pim neighbor 11.110.0.20 verbose
 Vpn-instance: public net
 Neighbor: 11.110.0.20
```

```
Interface: Ethernet1/2
Uptime: 00:00:10
Expiry time: 00:00:30
DR Priority: 1
Generation ID: 0x2ACEFE15
Holdtime: 105 s
LAN delay: 500 ms
Override interval: 2500 ms
State refresh interval: 60 s
Neighbor tracking: Disabled
```

display pim routing-table

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **routing-table** [*group-address* [**mask** { *mask-length* | *mask* }] | *source-address* [**mask** { *mask-length* | *mask* }] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

source-address: Multicast source address.

mask: Mask of the multicast group/source address, 255.255.255.255 by default.

mask-length: Mask length of the multicast group/source address, in the range of 0 to 32. The system default is 32.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**.

outgoing-interface: Displays routing entries of which the outgoing interface is the specified interface.

include: Displays routing entries of which the OIL includes the specified interface.

exclude: Displays routing entries of which the OIL does not include the specified interface.

match: Displays routing entries of which the OIL includes only the specified interface.

mode *mode-type*: Specifies a PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies PIM-DM.
- **sm**: Specifies PIM-SM.
- **ssm**: Specifies PIM-SSM.

flags *flag-value*: Displays routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **2msdp**: Specifies routing entries to be contained in the next SA message to notify an MSDP peer.
- **act**: Specifies multicast routing entries to which actual data has arrived.
- **del**: Specifies multicast routing entries scheduled to be deleted.
- **exprune**: Specifies multicast routing entries containing outgoing interfaces pruned by other multicast routing protocols.
- **ext**: Specifies routing entries containing outgoing interfaces contributed by other multicast routing protocols.
- **loc**: Specifies multicast routing entries on routers directly connecting to the same subnet with the multicast source.
- **msdp**: Specifies routing entries learned from MSDP SA messages.
- **niif**: Specifies multicast routing entries containing unknown incoming interfaces
- **nonbr**: Specifies routing entries with PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **rq**: Specifies multicast routing entries of the receiving side of the switch-MDT.
- **spt**: Specifies routing entries on the SPT.
- **sq**: Specifies multicast routing entries of the originator side of switch-MDT switchover.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description Use the **display pim routing-table** command to view PIM routing table information.

Related command: **display multicast routing-table** on page 1331.

Example # View the content of the PIM routing table in the public instance.

```
<Sysname> display pim routing-table
 Vpn-instance: public net
```

```
Total 0 (*, G) entry; 1 (S, G) entry

 (172.168.0.12, 227.0.0.1)
     RP: 2.2.2.2
     Protocol: pim-sm, Flag: SPT LOC ACT
     UpTime: 02:54:43
     Upstream interface: Ethernet1/0
         Upstream neighbor: NULL
         RPF prime neighbor: NULL
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: pim-sm, UpTime: 02:54:43, Expires: 00:02:47
```

Table 343 Description on the fields of the display pim routing-table command

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S, G) and (*, G) entries in the PIM routing table
(172.168.0.2, 227.0.0.1)	An (S, G) entry in the PIM routing table
Protocol	PIM mode, PIM-SM or PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the PIM routing table
Uptime	Length of time for which the (S, G) or (*, G) entry has been existing
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry ■ For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. ■ For an (S, G) entry, if this router directly connects to the multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	Information of the downstream interface(s), including: ■ Number of downstream interfaces ■ Downstream interface name ■ Protocol type on the downstream interface(s) ■ Uptime of the downstream interface(s) ■ Expiry time of the downstream interface(s)

display pim rp-info

Syntax **display pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **rp-info** [*group-address*]

View Any view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

group-address: Address of the multicast group of which the RP information is to be displayed, in the range of 224.0.1.0 to 239.255.255.255. If you do not provide a group address, this command will display the RP information corresponding to all multicast groups.

Description Use the **display pim rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Example # View the RP information corresponding to the multicast group 224.0.1.1 in the public instance.

```
<Sysname> display pim rp-info 224.0.1.1
 Vpn-instance: public net
 BSR RP Address is: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:10
     Expires: 00:02:30
 RP mapping for this group is: 2.2.2.2
```

View the RP information corresponding to all multicast groups in the public instance.

```
<Sysname> display pim rp-info
 Vpn-instance: public net
 PIM-SM BSR RP information:
 Group/MaskLen: 224.0.0.0/4
     RP: 2.2.2.2
     Priority: 0
     HoldTime: 150
     Uptime: 03:01:36
     Expires: 00:02:29
```

Table 344 Description on the fields of the display pim rp-info command

Field	Description
BSR RP Address is	IP address of the BSR RP
Group/MaskLen	The multicast group served by the RP
RP	IP address of the RP
Priority	RP priority
HoldTime	RP timeout time
Uptime	Length of time for which the RP has been up, in hours:minutes:seconds
Expires	Length of time in which the RP will expire, in hours:minutes:seconds

Table 344 Description on the fields of the display pim rp-info command

Field	Description
RP mapping for this group is: 2.2.2.2	The IP address of the RP serving the current multicast group is 2.2.2.2

hello-option dr-priority (PIM view)

Syntax **hello-option dr-priority** *priority*

undo hello-option dr-priority

View Public instance PIM view, VPN instance PIM view

Parameter *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

Related command: **pim hello-option dr-priority**.

Example # Set the router priority for DR election to 3 in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option dr-priority 3
```

hello-option holdtime (PIM view)

Syntax **hello-option holdtime** *interval*

undo hello-option holdtime

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **hello-option holdtime** command to configure the PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the default setting.

By default, the PIM neighbor timeout time is 105 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related command: **pim hello-option holdtime**.

Example # Set the global value of the PIM neighbor timeout time to 120 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option holdtime 120
```

hello-option lan-delay (PIM view)

Syntax **hello-option lan-delay** *interval*

undo hello-option lan-delay

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Prune delay in milliseconds, with an effective range of 1 to 32,767.

Description Use the **hello-option lan-delay** command to configure the global value of prune delay time, namely the length of time the device must wait upon receiving a prune message from downstream before taking the prune action. Within this period of time, if the device receives a prune override message from that downstream device, the prune action will be cancelled.

Use the **undo hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related command: **hello-option override-interval (PIM view)**, **pim hello-option override-interval**, and **pim hello-option lan-delay**.

Example # Set the prune delay to 200 milliseconds globally in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option lan-delay 200
```

hello-option neighbor-tracking (PIM view)

Syntax **hello-option neighbor-tracking**

undo hello-option neighbor-tracking

View Public instance PIM view, VPN instance PIM view

Parameter None

Description Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

This command is effective for both PIM-DM and PIM-SM.

Related command: **pim hello-option neighbor-tracking**.

Example # Disable join suppression globally in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option neighbor-tracking
```

hello-option override-interval (PIM view)

Syntax **hello-option override-interval** *interval*

undo hello-option override-interval

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

This command is effective for both PIM-DM and PIM-SM.

Related command: **hello-option lan-delay (PIM view)**, **pim hello-option lan-delay**, and **pim hello-option override-interval**.

Example # Set the prune override interval to 2,000 milliseconds globally in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] hello-option override-interval 2000
```

holdtime assert (PIM view)

Syntax **holdtime assert** *interval*

undo holdtime assert

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

This command is effective for both PIM-DM and PIM-SM.

Related command: **holdtime join-prune (PIM view)**, **pim holdtime join-prune**, and **pim holdtime assert**.

Example # Set the global value of the assert timeout time to 100 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime assert 100
```

holdtime join-prune (PIM view)

Syntax **holdtime join-prune** *interval*

undo holdtime join-prune

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

Related command: **holdtime assert (PIM view)**, **pim holdtime assert**, and **pim holdtime join-prune**.

Example # Set the global value of the join/prune timeout time to 280 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] holdtime join-prune 280
```

jp-pkt-size (PIM view)

Syntax **jp-pkt-size** *packet-size*

undo jp-pkt-size

View Public instance PIM view, VPN instance PIM view

Parameter *packet-size*: Maximum size of join/prune messages in bytes, with an effective range of 100 to 8,100.

Description Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the default setting.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related command: **jp-queue-size (PIM view)**.

Example # Set the maximum size of join/prune messages to 1,500 bytes in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-pkt-size 1500
```

jp-queue-size (PIM view)

Syntax **jp-queue-size** *queue-size*

undo jp-queue-size

View Public instance PIM view, VPN instance PIM view

Parameter *queue-size*: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

Description Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the default setting.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.
- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size (PIM view)**, **holdtime join-prune (PIM view)**, **pim holdtime join-prune**.

Example # Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] jp-queue-size 2000
```

pim

Syntax **pim** [**vpn-instance** *vpn-instance-name*]

undo pim [**vpn-instance** *vpn-instance-name*]

View System view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

Description Use the **pim** command to enter public instance PIM view or VPN instance PIM view.

Use the **undo pim** command to remove all configurations performed in public instance PIM view or VPN instance PIM view.

IP multicast must be enabled on the device before this command can take effect.

Related command: **multicast routing-enable** on page 1341.

Example # Enable IP multicast routing in the public instance and enter public instance PIM view.

```
<Sysname> system-view
[Sysname] multicast routing-enable
[Sysname] pim
[Sysname-pim]
```

Enable IP multicast routing in VPN instance mvpn and enter PIM view of VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] route-distinguisher 100:1
[Sysname-vpn-instance-mvpn] multicast routing-enable
[Sysname-vpn-instance-mvpn] quit
[Sysname] pim vpn-instance mvpn
[Sysname-pim-mvpn]
```

pim bsr-boundary

Syntax **pim bsr-boundary**

undo pim bsr-boundary

View Interface view

Parameter None

Description Use the **pim bsr-boundary** command to configure a BSR admin-scope region boundary on the current interface.

Use the **undo pim bsr-boundary** command to remove the configured BSR admin-scope region boundary.

By default, no BSR admin-scope region boundary is configured.

Related command: **c-bsr (PIM view)**, and **multicast boundary** on page 1337.

Example # Configure Ethernet 1/0 to be the boundary of the BSR admin-scope region.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim bsr-boundary
```

pim dm

Syntax **pim dm**

undo pim dm

View Interface view

Parameter None

Description Use the **pim dm** command to enable PIM-DM.

Use the **undo pim dm** command to disable PIM-DM.

By default, PIM-DM is disabled.

Note that PIM-DM cannot be used for multicast groups in the SSM group range.

Related command: **pim sm**, **ssm-policy (PIM view)**.

Example # Enable PIM-DM on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim dm
```

pim hello-option dr-priority

Syntax **pim hello-option dr-priority** *priority*

undo pim hello-option dr-priority

View Interface view

Parameter *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description Use the **pim hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

Related command: **hello-option dr-priority (PIM view)**.

Example # Set the router priority for DR election to 3 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim hello-option dr-priority 3
```

pim hello-option holdtime

Syntax **pim hello-option holdtime** *interval*

undo pim hello-option holdtime

View Interface view

Parameter *interval*: PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **pim hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim hello-option holdtime** command to restore the default setting.

By default, the PIM neighbor timeout time is 105 seconds.

Related command: **hello-option holdtime (PIM view)**.

Example # Set the PIM neighbor timeout time to 120 seconds on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim hello-option holdtime 120
```

pim hello-option lan-delay

Syntax **pim hello-option lan-delay** *interval*

undo pim hello-option lan-delay

View Interface view

Parameter *interval*: Prune delay in milliseconds, with an effective range of 1 to 32,767.

Description Use the **pim hello-option lan-delay** command to configure the prune delay time on the current interface.

Use the **undo pim hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

Related command: **pim hello-option override-interval**, **hello-option override-interval (PIM view)**, and **hello-option lan-delay (PIM view)**.

Example # Set the prune delay time to 200 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim hello-option lan-delay 200
```

pim hello-option neighbor-tracking

Syntax **pim hello-option neighbor-tracking**

undo pim hello-option neighbor-tracking

View Interface view

Parameter None

Description Use the **pim hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related command: **hello-option neighbor-tracking (PIM view)**.

Example # Disable join suppression on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim hello-option neighbor-tracking
```

pim hello-option override-interval

Syntax **pim hello-option override-interval** *interval*

undo pim hello-option override-interval

View Interface view

Parameter *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description Use the **pim hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

Related command: **pim hello-option lan-delay**, **hello-option lan-delay (PIM view)**, and **hello-option override-interval (PIM view)**.

Example # Set the prune override interval to 2,000 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim hello-option override-interval 2000
```

pim holdtime assert

Syntax **pim holdtime assert** *interval*

undo pim holdtime assert

View Interface view

Parameter *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description Use the **pim holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

Related command: **holdtime join-prune (PIM view)**, **pim holdtime join-prune**, and **holdtime assert (PIM view)**.

Example # Set the assert timeout time to 100 seconds on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim holdtime assert 100
```

pim holdtime join-prune

Syntax **pim holdtime join-prune** *interval*

undo pim holdtime join-prune

View Interface view

Parameter *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **pim holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

Related command: **holdtime assert (PIM view)**, **pim holdtime assert**, and **holdtime join-prune (PIM view)**.

Example # Set the join/prune timeout time to 280 seconds on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim holdtime join-prune 280
```

pim require-genid

Syntax **pim require-genid**

undo pim require-genid

View Interface view

Parameter None

Description Use the **pim require-genid** command enable rejection of hello messages without Generation_ID.

Use the **undo pim require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Example # Enable Ethernet1/0 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim require-genid
```

pim sm

Syntax **pim sm**

undo pim sm

View Interface view

Parameter None

Description Use the **pim sm** command to enable PIM-SM.

Use the **undo pim sm** command to disable PIM-SM.

By default, PIM-SM is disabled.

Related command: **pim dm**.

Example # Enable PIM-SM on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim sm
```

pim state-refresh-capable

Syntax **pim state-refresh-capable**

undo pim state-refresh-capable

View Interface view

Parameter None

Description Use the **pim state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related command: **state-refresh-interval (PIM view)**, **state-refresh-rate-limit (PIM view)**, and **state-refresh-ttl (PIM view)**.

Example # Disable state refresh on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo pim state-refresh-capable
```

pim timer graft-retry

Syntax **pim timer graft-retry** *interval*

undo pim timer graft-retry

View Interface view

Parameter *interval*: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description Use the **pim timer graft-retry** command to configure the graft retry period.

Use the **undo pim timer graft-retry** command to restore the default setting.

By default, the graft retry period is 3 seconds.

Example # Set the graft retry period to 80 seconds on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim timer graft-retry 80
```

pim timer hello

Syntax **pim timer hello** *interval*

undo pim timer hello

View Interface view

Parameter *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **pim timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

Related command: **timer hello (PIM view)**.

Example # Set the hello interval to 40 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim timer hello 40
```

pim timer join-prune

Syntax **pim timer join-prune** *interval*

undo pim timer join-prune

View Interface view

Parameter *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **pim timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

Related command: **timer join-prune (PIM view)**.

Example # Set the join/prune interval to 80 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim timer join-prune 80
```

pim triggered-hello-delay

Syntax **pim triggered-hello-delay** *interval*

undo pim trigged-hello-delay

View Interface view

Parameter *interval*: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

Description Use the **pim triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim triggered-hello-delay** command to restore the default setting.

By default, the maximum delay between hello messages is 5 seconds.

Example # Set the maximum delay between hello messages to 3 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim trigged-hello-delay 3
```

probe-interval (PIM view)

Syntax **probe-interval** *interval*

undo probe-interval

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Register probe time in seconds, with an effective range of 1 to 3,600.

Description Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the default setting.

By default, the register probe time is 5 seconds.

Related command: **register-suppression-timeout (PIM view)**.

Example # Set the probe time to 6 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] probe-interval 6
```

register-policy (PIM view)

Syntax **register-policy** *acl-number*

undo register-policy

View Public instance PIM view, VPN instance PIM view

Parameter *acl-number*: Advanced ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the ACL can be accepted by the RP.

Description Use the **register-policy** command to configure an ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related command: **register-suppression-timeout (PIM view)**.

Example # In the public instance configure the RP to accept only those register messages for multicast traffic from multicast sources in the range of 10.10.0.0/16 to multicast groups in the range of 225.1.0.0/16.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule permit ip source 10.10.0.0 0.0.255.255 d
estination 225.1.0.0 0.0.255.255
[Sysname-acl-adv-3000] quit
[Sysname] pim
[Sysname-pim] register-policy 3000
```

register-suppression-timeout (PIM view)

Syntax **register-suppression-timeout** *interval*

undo register-suppression-timeout

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Register suppression timeout in seconds, in the range of 1 to 3,600.

Description Use the **register-suppression-timeout** command to configure the register suppression timeout time.

Use the **undo register-suppression-timeout** command to restore the default setting.

By default, the register suppression timeout time is 60 seconds.

Related command: **probe-interval (PIM view)** and **register-policy (PIM view)**.

Example # Set the register suppression timeout time to 70 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-suppression-timeout 70
```

register-whole-checksum (PIM view)

Syntax **register-whole-checksum**

undo register-whole-checksum

View Public instance PIM view, VPN instance PIM view

Parameter None

Description Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based on the header in the register message.

Related command: **register-policy (PIM view)** and **register-suppression-timeout (PIM view)**.

Example # Configure the router to calculate the checksum based on the entire register message in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] register-whole-checksum
```

reset pim control-message counters

Syntax **reset pim** [**vpn-instance** *vpn-instance-name* | **all-instance**] **control-message counters** [**interface** *interface-type interface-number*]

View User view

Parameter *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

all-instance: Specifies all VPN instances.

interface *interface-type interface-number*: Specifies to reset the PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information of PIM control messages on all interfaces.

Description Use the **reset pim control-message counters** command to reset PIM control message counters.

Example # Reset PIM control message counters on all interfaces in the public instance.

```
<Sysname> reset pim control-message counters
```

source-lifetime (PIM view)

Syntax **source-lifetime** *interval*

undo source-lifetime

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Multicast source lifetime in seconds, with an effective range of 1 to 65,535.

Description Use the **source-lifetime** command to configure the multicast source lifetime.

Use the **undo source-lifetime** command to restore the default setting.

By default, the lifetime of a multicast source is 210 seconds.

Related command: **state-refresh-interval (PIM view)**.

Example # Set the multicast source lifetime to 200 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] source-lifetime 200
```

source-policy (PIM view)

Syntax **source-policy** *acl-number*

undo source-policy

View Public instance PIM view, VPN instance PIM view

Parameter *acl-number*: Basic or advanced ACL number, in the range of 2000 to 3999.

Description Use the **source-policy** command to configure a multicast data filter.

Use the **undo source-policy** command to remove the configured multicast data filter.

By default, no multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received multicast packets based on the source address, and discards packets that fail the source address match.
- If you specify an advanced ACL, the device filters all the received multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Example # In the public instance configure the router to accept multicast packets originated from 10.10.1.2 and discard multicast packets originated from 10.10.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.10.1.2 0
[Sysname-acl-basic-2000] rule deny source 10.10.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] source-policy 2000
```

spt-switch-threshold (PIM view)

Syntax **spt-switch-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl-number*]

View Public instance PIM view, VPN instance PIM view

Parameter *traffic-rate*: Traffic rate threshold that will trigger RPT-to-SPT switchover, in units of kbps. The effective range is 1 to 4,194,304.

infinity: Disables RPT-to-SPT switchover.

group-policy *acl-number*: Uses this threshold for multicast groups matching the specified multicast policy. In this option, *acl-number* refers to a basic ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the threshold will apply on all multicast groups.

order *order-value*: Specifies the order of the ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the ACL in the group-policy list. If you have assigned an *order-value* to a certain ACL, do not specify the same *order-value* for another ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the ACL will remain the same in the group-policy list.

Description Use the **spt-switch-threshold** command to configure the RPT-to-SPT switchover parameters.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first multicast packet from the RPT.

Note that:

- To adjust the order of an existing ACL in the group-policy list, you can use the *acl-number* argument to specify this ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. The order of the other existing ACLs in the group-policy list will remain unchanged.
- To use an ACL that does not exist in the group-policy list, you can use the *acl-number* argument to specify an ACL and set its *order-value*. This will insert the ACL to the position of *order-value* in the group-policy list. If you do not include the **order** *order-value* option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same multicast group, the first traffic rate configuration matched in sequence will take effect.

Example # Set the traffic rate threshold to trigger RPT-to-SPT switchover to 4 kbps in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold 4
```

In the public instance create a group-policy with the ACL number of 2010 and the traffic rate threshold of 100 kbps, and insert the ACL to the first position.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] spt-switch-threshold 100 group-policy 2010 order 1
```

ssm-policy (PIM view)

Syntax **ssm-policy** *acl-number*

undo ssm-policy

View Public instance PIM view, VPN instance PIM view

Parameter *acl-number*: Basic ACL number, in the range of 2000 to 2999.

Description Use the **ssm-policy** command to configure the SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the SSM group range is 232.0.0.0/8.

This command allows you to define an address range of permitted or denied multicast sources or groups. If the match succeeds, the multicast mode will be PIM-SSM; otherwise the multicast mode will be PIM-SM.

Example # Configure the SSM group range to be 232.1.0.0/16 in the public instance.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 232.1.0.0 0.0.255.255
[Sysname-acl-basic-2000] quit
[Sysname] pim
[Sysname-pim] ssm-policy 2000
```

state-refresh-interval (PIM view)

Syntax **state-refresh-interval** *interval*

undo state-refresh-interval

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: State refresh interval in seconds, with an effective range of 1 to 255.

Description Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the default setting.

By default, the state refresh interval is 60 seconds.

Related command: **pim state-refresh-capable**, **state-refresh-rate-limit (PIM view)**, and **state-refresh-ttl (PIM view)**.

Example # Set the state refresh interval to 70 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-interval 70
```

state-refresh-rate-limit (PIM view)

Syntax **state-refresh-rate-limit** *interval*

undo state-refresh-rate-limit

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the default setting.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related command: **pim state-refresh-capable**, **state-refresh-interval (PIM view)**, and **state-refresh-ttl (PIM view)**.

Example # In the public instance configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-rate-limit 45
```

state-refresh-ttl (PIM view)

Syntax **state-refresh-ttl** *ttl-value*

undo state-refresh-ttl

View Public instance PIM view, VPN instance PIM view

Parameter *ttl-value*: TTL value of state refresh messages, in the range of 1 to 255.

Description Use the **state-refresh-ttl** command to configure the TTL value of state refresh messages.

Use the **undo state-refresh-ttl** command to restore the default setting.

By default, the TTL value of state refresh messages is 255.

Related command: **pim state-refresh-capable**, **state-refresh-interval (PIM view)**, and **state-refresh-rate-limit (PIM view)**.

Example # In the public instance configure the device to send PIM state refresh messages with a TTL of 45.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] state-refresh-ttl 45
```

static-rp (PIM view)

Syntax **static-rp** *rp-address* [*acl-number*] [**preferred**]

undo static-rp *rp-address*

View Public instance PIM view, VPN instance PIM view

Parameter *rp-address*: IP address of the static RP to be configured. This address must be a legal unicast IP address, rather than an address on the 127.0.0.0/8 segment.

acl-number: Basic ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those groups that pass the ACL filtering; otherwise, the configured static RP will serve the all-system group 224.0.0.0/4.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect on if no dynamic RP exists in the network or when the dynamic RP fails.

Description Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- PIM-SM or PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the ACL rule applied on a static RP changes, a new RP must be elected for all the multicast groups.
- You can configure multiple static RPs by using this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same multicast group, the one with the highest IP address will be chosen to serve the multicast group.

- You can configure up to 50 static RPs on the same device.

Related command: **display pim rp-info** and **auto-rp enable**.

Example # In the public instance, configure the interface with the IP address 11.110.0.6 to be a static RP that serves the multicast groups defined in ACL 2001, and give priority to this static RP in the case of static/dynamic RP conflict.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] static-rp 11.110.0.6 2001 preferred
```

timer hello (PIM view)

Syntax **timer hello** *interval*

undo timer hello

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

Related command: **pim timer hello**.

Example # Set the global hello interval to 40 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer hello 40
```

timer join-prune (PIM view)

Syntax **timer join-prune** *interval*

undo timer join-prune

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

Related command: **pim timer join-prune**.

Example # Set the global join/prune interval to 80 seconds in the public instance.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer join-prune 80
```

timer spt-switch (PIM view)

Syntax **timer spt-switch** *interval*

undo timer spt-switch

View Public instance PIM view, VPN instance PIM view

Parameter *interval*: Interval in seconds between checks of the traffic rate threshold prior to RPT-to-SPT switchover, in the range of 15 to 65,535.

Description Use the **timer spt-switch** command to configure the interval between checks of the traffic rate threshold before RPT-to-SPT switchover.

Use the **undo timer spt-switch** command to restore the default setting.

By default, the traffic rate threshold is checked at an interval of 15 seconds before RPT-to-SPT switchover.

Before using this command, be sure to use the **spt-switch-threshold** command to configure the traffic rate threshold that should trigger RPT-to-SPT switchover. Otherwise, the interval set in this command will be meaningless.

Related command: **spt-switch-threshold (PIM view)**.

Example # In the public instance set the interval between checks of the traffic rate threshold prior to RPT-to-SPT switchover to 30 seconds.

```
<Sysname> system-view
[Sysname] pim
[Sysname-pim] timer spt-switch 30
```

91 IPv6 Multicast Routing and Forwarding Configuration Commands

display multicast ipv6 boundary

Syntax **display multicast ipv6 boundary** [*ipv6-group-address* [*prefix-length*] | **interface** *interface-type interface-number*]

View Any view

Parameter *ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of the IPv6 multicast group address, in the range of 8 to 128. The system default is 128.

interface-type interface-number: Interface type and interface number.

Description Use the **display multicast ipv6 boundary** command to display the IPv6 multicast boundary information on the specified interface or all interfaces.

Related command: **multicast ipv6 boundary**.

Example # Display the IPv6 multicast boundary information configured on all interfaces.

```
<Sysname> display multicast ipv6 boundary
IPv6 multicast boundary information
 Boundary            Interface
 FF03::/16           Eth1/0
 FF09::/16           Pos5/0
```

Table 345 Description on the fields of the display multicast ipv6 boundary command

Field	Description
Boundary	IPv6 multicast group corresponding to the IPv6 multicast boundary
Interface	Boundary interface corresponding to the IPv6 multicast boundary

display multicast ipv6 forwarding-table

Syntax **display multicast ipv6 forwarding-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } } | **statistics**] [**port-info**]

View Any view

Parameter *ipv6-source-address*: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of the IPv6 multicast group/source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays the routing entries whose incoming interface is the specified ones.

interface-type interface-number: Interface type and interface number.

register: Represents a registered interface.

outgoing-interface: Displays the routing entries whose outgoing interface is the specified ones.

exclude: Displays the routing entries whose outgoing interface list (OIL) excludes the specified interface.

include: Displays the routing entries whose OIL includes the specified interface.

match: Displays the routing entries whose OIL includes and includes only the specified interface.

statistics: Specifies to display the statistics information of the IPv6 multicast forwarding table.

port-info: Displays Layer 2 port information.

Description Use the **display multicast ipv6 forwarding-table** command to display information of an IPv6 multicast forwarding table.

Related command: **multicast ipv6 forwarding-table downstream-limit**, **multicast ipv6 forwarding-table route-limit**, and **display multicast ipv6 routing-table**.

Example # Display information of an IPv6 multicast forwarding table.

```
IPv6 Multicast Forwarding Table
Total 1 entry

Total 1 entry matched

00001. (2000:5::1:1000, FF1E::1234)
     MID: 0, Flags: 0x0:0
     Uptime: 04:04:37, Timeout in: 00:03:26
     Incoming interface: Ethernet1/0
     List of 1 outgoing interfaces:
       1: Ethernet1/1
```

```
Matched 146754 packets(10272780 bytes), Wrong If 0 packets
Forwarded 139571 packets(9769970 bytes)
```

Table 346 Description on the fields of the display multicast ipv6 forwarding-table command

Field	Description
00001	Sequence number if the (S, G) entry
(2000:5::1:1000, FF1E::1234)	(S, G) entry in the IPv6 multicast forwarding table
MID	(S, G) entry ID. Each (S, G) entry has a unique MID
Flags	Current state of a (S, G) entry. Different bits are used to indicate different states of the (S, G) entry. For the values and meanings of this field, see Table 347.
Uptime	Length of time the (S, G) entry has been up
Timeout in	Length of time in which the (S, G) entry will time out
Incoming interface	Incoming interface of a (S, G) entry
List of 1 outgoing interfaces:	1 outgoing interface list:
1: Ethernet1/1	Sequence number of outgoing interface: outgoing interface type and number
Matched 146754 packets(10272780 bytes), Wrong If 0 packets	Number of matched packets (number of bytes), number of packets with incoming interface errors
Forwarded 139571 packets(9769970 bytes)	Number of forwarded IPv6 multicast packets (number of bytes)

Table 347 Values and meanings of the Flags field

Value	Meaning
0x00000001	Indicates that a register-stop message needs to be sent.
0x00000002	Indicates whether the IPv6 multicast source corresponding to the (S, G) entry is active.
0x00000004	Indicates a null forwarding entry.
0x00000008	Indicates whether the RP is a border router in an IPv6 PIM domain.
0x00000010	Indicates a register outgoing interface is available
0x00000400	Indicates an entry to be deleted
0x00008000	Indicates that the (S, G) entry is in smoothening process after active/standby switchover
0x00010000	Indicates that the (S, G) entry has been updated during the smoothening process.
0x00080000	Indicates that the (S, G) entry has been repeatedly updated and need to be deleted before adding a new entry is added.
0x00100000	Indicates that a (S, G) entry is added successfully

display multicast ipv6 minimum-hoplimit

Syntax **display multicast ipv6 minimum-hoplimit** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command will display the minimum hop limit required for an IPv6 multicast packet to be forwarded on all interfaces.

Description Use the **display multicast ipv6 minimum-hoplimit** command to view the minimum hop limit required for an IPv6 multicast packet to be forwarded on the specified interface or all interfaces.

Related command: **multicast ipv6 minimum-hoplimit**.

Example # Display the minimum hop limit required for an IPv6 multicast packet to be forwarded on all interfaces.

```
<Sysname> display multicast ipv6 minimum-hoplimit
IPv6 multicast Hop Limit information
 Interface           Hop Limit
 Eth1/0              5
 Eth1/1              6
```

Table 348 Description on the fields of the display multicast ipv6 minimum-hoplimit command

Field	Description
Interface	Interface name
Hop Limit	Minimum hop limit value required for an IPv6 multicast packet to be forwarded on the interface

display multicast ipv6 routing-table

Syntax **display multicast ipv6 routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } | **outgoing-interface** { { **exclude** | **include** | **match** } { *interface-type interface-number* | **register** } }] *

View Any view

Parameter *ipv6-source-address*: Multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of the multicast group/source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Displays routing entries whose incoming interface is the specified one.

interface-type interface-number: Interface type and interface number.

register: Represents a registered interface.

outgoing-interface: Displays routing entries whose outgoing interface is the specified ones.

exclude: Displays routing entries whose OIL excludes the specified interface.

include: Displays routing entries whose OIL includes the specified interface.

match: Displays routing entries whose OIL includes only the specified interface.

Description Use the **display multicast ipv6 routing-table** command to display the information of an IPv6 multicast routing table.

Related command: **display multicast ipv6 forwarding-table**.

Example # Display the information of an IPv6 multicast routing table.

```
<Sysname> display multicast ipv6 routing-table
IPv6 multicast routing table
 Total 1 entry

 00001. (2001::2, FFE3::101)
       Uptime: 00:00:14
       Upstream Interface: Ethernet1/0
       List of 1 downstream interface
           1:  Ethernet1/1
```

Table 349 Description on the fields of the display multicast ipv6 routing-table command

Field	Description
00001	Sequence number of the (S, G) entry
(2001::2, FFE3::101)	(S, G) entry in an IPv6 multicast forwarding table
Uptime	Length of time a (S, G) entry has been up.
Upstream interface	Upstream interface of a (S, G) entry. Multicast packets should arrive through this interface
List of 2 downstream interfaces	Downstream interface list. These interfaces need to forward multicast packets.

display multicast ipv6 rpf-info

Syntax **display multicast ipv6 rpf-info** *ipv6-source-address* [*ipv6-group-address*]

View Any view

Parameter *ipv6-source-address*: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number from 0 to F.

Description Use the command to display RPF information of an IPv6 multicast source.

Related command: **display multicast ipv6 routing-table** and **display multicast ipv6 forwarding-table**.

Example # Display all RPF information of the multicast source with an IPv6 address 2001::101.

```
<Sysname> display multicast ipv6 rpf-info 2001::101
 RPF information about source 2001::101:
     RPF interface: Ethernet1/0, RPF neighbor: 2002::201
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     Route selection rule: preference-preferred
     Load splitting rule: disable
```

Table 350 Description on the fields of the display multicast ipv6 rpf-info command

Field	Description
RPF information about source 2001::101	RPF information of the IPv6 multicast source 2001::101
RPF interface	RPF interface
RPF neighbor	IPv6 address of the RPF neighbor
Referenced prefix/prefix length	Referenced route and prefix length
Referenced route type	Type of the referenced route, which can be any of the following: ■ igp: IPv6 unicast route (IGB) ■ egp: IPv6 unicast (EGP) ■ unicast (direct): IPv6 unicast route (directly connected) ■ unicast: other IPv6 unicast route (such as IPv6 unicast static route)
Route selection rule	RPF route selection rule: An RPF route can be selected by the priority of the routing protocol or by the longest match of the destination address in the routing table.
Load splitting rule	Load sharing rule

multicast ipv6 boundary

Syntax **multicast ipv6 boundary** *ipv6-group-address prefix-length*

undo multicast ipv6 boundary { *ipv6-group-address prefix-length* | **all** }

View Interface view

Parameter *ipv6-group-address*: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 through F.

prefix-length: Prefix length of the IPv6 multicast group address, in the range of 8 to 128.

all: Deletes all IPv6 multicast boundaries configured on the interface.

Description Use the **multicast ipv6 boundary** command to configure an IPv6 multicast forwarding boundary.

Use the **undo multicast ipv6 boundary** command to delete a specified IPv6 multicast forwarding boundary or all IPv6 multicast forwarding boundaries.

By default, no multicast forwarding boundary is configured.

Note that:

- A multicast forwarding boundary sets the boundary condition for the IPv6 multicast groups in the specified range. If the destination address of an IPv6 multicast packet matches the set boundary condition, the packet will not be forwarded.
- If an interface needs to act as a forwarding boundary for multiple IPv6 multicast groups, just carry out this command on the interface once for each group.
- Assume that Set A and Set B are both multicast forwarding boundary sets to be configured, and that B is a subset of A. If A has been configured on an interface, it is not allowed to configure B on the interface; if B has been configured on the interface before A is configured, the previously configured B will be removed.

Related command: **display multicast ipv6 boundary**.

Example # Configure Ethernet 1/0 to be the forwarding boundary of the IPv6 multicast group FF03::101/16.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] multicast ipv6 boundary FF03::101 16
```

multicast ipv6 forwarding-table downstream-limit

Syntax **multicast ipv6 forwarding-table downstream-limit** *limit*

undo multicast ipv6 forwarding-table downstream-limit

View System view

Parameter *limit*: Maximum number of downstream nodes (namely the maximum number of outgoing interfaces) for a single route in the IPv6 multicast forwarding table. The value ranges from 0 to 128.

Description Use the **multicast ipv6 forwarding-table downstream-limit** command to configure the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table downstream-limit** command to restore the system default.

By default, the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table is 128.

Related command: **display multicast ipv6 forwarding-table**.

Example # Set the maximum number of downstream nodes for a single route in the IPv6 multicast forwarding table to 120.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table downstream-limit 120
```

multicast ipv6 forwarding-table route-limit

Syntax **multicast ipv6 forwarding-table route-limit** *limit*

undo multicast ipv6 forwarding-table route-limit

View System view

Parameter *limit*: Maximum number of routing entries in the IPv6 multicast forwarding table. The value ranges 0 to 900.

Description Use the **multicast ipv6 forwarding-table route-limit** command to configure the maximum number of routing entries in the IPv6 multicast forwarding table.

Use the **undo multicast ipv6 forwarding-table route-limit** command to restore the maximum number of routing entries in the IPv6 multicast forwarding table to the system default.

By default, the maximum number of routing entries in the IPv6 multicast forwarding table is 900.

The allowable maximum number of routing entries varies with devices.

Related command: **display multicast ipv6 forwarding-table**.

Example # Set the maximum number of routing entries in the IPv6 multicast forwarding table to 200.

```
<Sysname> system-view
[Sysname] multicast ipv6 forwarding-table route-limit 200
```

multicast ipv6 load-splitting

Syntax **multicast ipv6 load-splitting** {**source** | **source-group** }

undo multicast ipv6 load-splitting

View System view

Parameter **source**: Specifies to implement IPv6 multicast load splitting on a per-source basis.

source-group: Specifies to implement IPv6 multicast load splitting on a per-source and per-group basis.

Description Use the **multicast load-splitting** command to enable load splitting of IPv6 multicast traffic.

Use the **undo multicast load-splitting** command to disable load splitting of IPv6 multicast traffic.

By default, load splitting of IPv6 multicast traffic is disabled.

Example # Enable load splitting of IPv6 multicast traffic on a per-source basis.

```
<Sysname> system-view
[Sysname] multicast ipv6 load-splitting source
```

multicast ipv6 longest-match

Syntax **multicast ipv6 longest-match**

undo multicast ipv6 longest-match

View System view

Parameter None

Description Use the **multicast ipv6 longest-match** command to configure route selection based on the longest match, namely based on the prefix length.

Use the **undo multicast ipv6 longest-match** command to remove the configuration of route selection based on the longest match.

By default, routes are selected in order of routing entries.

Example # Configure route selection based on the longest match.

```
<Sysname> system-view
[Sysname] multicast ipv6 longest-match
```

multicast ipv6 minimum-hoplimit

Syntax **multicast ipv6 minimum-hoplimit** *ttl-value*

undo multicast ipv6 minimum-hoplimit

View Interface view

Parameter *hoplimit-value*: Minimum hop limit required for an IPv6 multicast packet to be forwarded on the interface, in the range of 1 to 255.

Description Use the **multicast ipv6 minimum-hoplimit** command to configure the minimum hop limit required for an IPv6 multicast packet to be forwarded.

Use the **undo multicast minimum-hoplimit** command to restore the system default.

By default, the minimum hop limit required for an IPv6 multicast packet to be forwarded is 1.

Related command: **display multicast ipv6 minimum-hoplimit**.

Example # Set the minimum hop limit required for an IPv6 multicast packet to be forwarded by Ethernet 1/0 to 8.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] multicast ipv6 minimum-hoplimit 8
```

multicast ipv6 routing-enable

Syntax **multicast ipv6 routing-enable**

undo multicast ipv6 routing-enable

View System view

Parameter None

Description Use the **multicast ipv6 routing-enable** command to enable IPv6 multicast routing.

Use the **undo multicast ipv6 routing-enable** command to disable IPv6 multicast routing.

IPv6 multicast routing is disabled by default.

Note that:

- You must enable IPv6 multicast routing before you can carry out other Layer 3 IPv6 multicast commands.
- The device does not forward any IPv6 multicast packets before IPv6 multicast routing is enabled.

Example # Enable IPv6 multicast routing.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
```

reset multicast ipv6 forwarding-table

Syntax **reset multicast ipv6 forwarding-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameter *ipv6-source-address*: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Prefix length of the IPv6 multicast group/source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128; for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Specifies to clear IPv6 multicast forwarding entries of which the incoming interface is the specified one.

interface-type interface-number: Interface type and interface number.

register: Specifies the register interface.

all: Clears all forwarding entries from the IPv6 multicast forwarding table.

Description Use the **reset multicast ipv6 forwarding-table** command to clear forwarding entries from the IPv6 multicast forwarding table.

When a forwarding entry is deleted from the IPv6 multicast forwarding table, the corresponding routing entry is also deleted from the IPv6 multicast routing table.

Related command: **reset multicast IPv6 routing-table**, **display multicast ipv6 routing-table**, and **display multicast ipv6 forwarding-table**.

Example # Clear the IPv6 multicast forwarding entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast forwarding table.

```
<Sysname> reset multicast ipv6 forwarding-table ff03::101
```

reset multicast IPv6 routing-table

Syntax **reset multicast ipv6 routing-table** { { *ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*] | **incoming-interface** { *interface-type interface-number* | **register** } } * | **all** }

View User view

Parameter *ipv6-source-address*: IPv6 multicast source address.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16, where x and y represent any hexadecimal number from 0 to F.

prefix-length: Prefix length of the IPv6 multicast group/source address. For an IPv6 multicast group address, this argument has an effective value range of 8 to 128 for an IPv6 multicast source address, this argument has an effective value range of 0 to 128. The system default is 128 in both cases.

incoming-interface: Clears IPv6 multicast routing entries of which the incoming interface is the specified one.

interface-type interface-number: Interface type and interface number.

register: Specifies a registration interface.

all: Clears all routing entries from the IPv6 multicast routing table.

Description Use the **reset multicast ipv6 routing-table** command to clear IPv6 routing entries from the IPv6 multicast routing table.

When a routing entry is deleted from the IPv6 multicast routing table, the corresponding forwarding entry is also deleted from the IPv6 multicast forwarding table.

Related command: **reset multicast ipv6 forwarding-table**, **display multicast ipv6 forwarding-table** and **display multicast ipv6 routing-table**.

Example # Clear the routing entries related to the IPv6 multicast group FF03::101 from the IPv6 multicast routing table.

```
<Sysname> reset multicast ipv6 routing-table ff03::101
```

92 MLD CONFIGURATION COMMANDS

display mld group

Syntax **display mld group** [*ipv6-group-address* | **interface** *interface-type interface-number*] [**static** | **verbose**]

View Any view

Parameter *ipv6-group-address*: MLD multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y::), where x and y represent any hexadecimal number ranging from 0 to F.

interface *interface-type interface-number*: Displays the information of MLD multicast groups on the specified interface.

static: Displays the information of statically joined MLD multicast groups.

verbose: Displays detailed information of MLD multicast groups.

Description Use the **display mld group** command to view information of MLD multicast groups.

Note that:

- If you do not specify an IPv6 multicast group address, this command will display the MLD information of all the multicast groups.
- If you do not specify *interface-type interface-number*, this command will display the MLD multicast group information on all the interfaces.
- If you do not specify the **static** keyword, the information of only dynamically joined MLD groups will be displayed.

Example # View the detailed information of dynamically joined MLD multicast groups on all interfaces.

```
<Sysname> display mld group verbose
Interface group report information
Ethernet1/0(FE80::101)
  Total 1 MLD Groups reported
   Group: FF03::101
     Uptime: 00:01:46
     Expires: 00:01:30
     Last reporter: FE80::10
     Last-listener-query-counter: 0
```

```
Last-listener-query-timer-expiry: off
Group mode: include
Version1-host-present-timer-expiry: off
```

Table 351 Description on the fields of the display mld group command

Field	Description
Group	IPv6 multicast group address
Uptime	Length of time since the IPV6 multicast group was joined
Expires	Remaining time of the IPv6 multicast group
Last reporter	IPv6 address of the host that last reported membership for this group
Last-listener-query-counter	Number of MLD multicast-address-specific queries sent
Last-listener-query-timer-expiry	Remaining time of the MLD last listener query timer
Group mode	Filtering mode of multicast sources
Version1-host-present-timer-expiry	Remaining time of the MLDv1 host present timer

display mld interface

Syntax **display mld interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number. If you do not specify an interface, this command will display the information of all interfaces running MLD.

verbose: Displays detailed MLD configuration and operation information.

Description Use the **display mld interface** command to view MLD configuration and operation information on the specified interface or all MLD-enabled interfaces.

Example # View the detailed MLD configuration and operation information on Ethernet 1/0.

```
<Sysname> display mld interface ethernet 1/0 verbose
Ethernet1/0(FE80::200:AFF:FE01:101):
   MLD is enabled
   Current MLD version is 2
   Value of query interval for MLD(in seconds): 125
   Value of other querier present interval for MLD(in seconds): 255
   Value of maximum query response time for MLD(in seconds): 10
     Value of startup query interval(in seconds): 31
   Value of startup query count: 2
   General query timer expiry (hours:minutes:seconds): 00:00:23
   Querier for MLD: FE80::200:AFF:FE01:101 (this router)
   MLD activity: 1 joins, 0 leaves
   Multicast ipv6 routing on this interface: enabled
   Robustness: 2
   Require-router-alert: disabled
```

```
Fast-leave: disabled
Startup-query-timer-expiry: off
Other-querier-present-timer-expiry: off
```

Table 352 Description on the fields of the display mld group port-info command

Field	Description
Ethernet1/0(FE80::200:AFF:FE01:101):	Interface name (IPv6 link-local address)
Current MLD version	MLD version running on the interface
MLD group policy	MLD group policy
Value of query interval for MLD (in seconds)	MLD query interval, in seconds
Value of other querier present interval for MLD (in seconds)	MLD other querier present interval, in seconds
Value of maximum query response time for MLD (in seconds)	Maximum response delay for general query messages (in seconds)
Value of last listener query interval (in seconds)	MLD last listener query interval, in seconds
Value of startup query interval(in seconds)	MLD startup query interval, in seconds
Value of startup query count	Number of MLD general queries sent on startup
General query timer expiry	Remaining time of the MLD general query timer
Querier for MLD	IPv6 link-local address of the MLD querier
MLD activity	MLD activity statistics (join and done messages)
Robustness	MLD querier robustness variable
Require-router-alert	Whether to discard MLD packets without the Router-Alert option
Fast-leave	Indicates whether MLD fast leave processing is enabled
Startup-query-timer-expiry	Remaining time of MLD startup query timer
Other-querier-present-timer-expiry	Remaining time of the MLD other querier present timer

display mld routing-table

Syntax **display mld routing-table** [*ipv6-source-address* [*prefix-length*] | *ipv6-group-address* [*prefix-length*]] *

View Any view

Parameter *ipv6-source-address*: Specifies a multicast source by its IPv6 address.

ipv6-group-address: Specifies an IPv6 multicast group by its IPv6 address, in the format of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

prefix-length: Prefix length of the multicast source or multicast group address. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description Use the **display mld routing-table** command to view the MLD routing table information.

Example # View the information of the MLD routing table.

```
<Sysname> display mld routing-table
Routing table
 Total 1 entry

 00001. (*, FF1E::101)
       List of 1 downstream interface
        Ethernet1/0 (FE80::200:5EFF:FE71:3800),
                    Protocol: MLD
```

Table 353 Description on the fields of the display mld routing-table command

Field	Description
00001	Sequence number this (*, G) entry
(*, FF1E::101)	A (*, G) entry in the MLD routing table
List of 1 downstream interface	List of downstream interfaces, namely the interfaces to which the multicast data for this group be forwarded

fast-leave (MLD view)

Syntax **fast-leave** [**group-policy** *acl6-number*]

undo fast-leave

View MLD view

Parameter *acl6-number*: Number of a basic IPv6 ACL, in the range of 2000 to 2999.

Description Use the **fast-leave** command to enable the fast-leave feature globally.

Use the **undo fast-leave** command to disable the fast-leave feature globally.

By default, the fast-leave feature is disabled, that is, the MLD querier sends a multicast-address-specific query upon receiving an MLD done message from a host, instead of sending a leave notification directly to the upstream.

Related command: **mld fast-leave** and **last-listener-query-interval**.

This command takes effect on all Layer 3 interfaces when executed in MLD view.

Example # Enable the fast-leave function for IPv6 multicast group members globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] fast-leave
```

last-listener-query-interval

Syntax **last-listener-query-interval** *interval*

undo last-listener-query-interval

View MLD view

Parameter *interval*: Last listener query interval in seconds, in the range of 1 to 5.

Description Use the **last-listener-query-interval** command to configure the last listener query interval globally.

Use the **undo last-listener-query-interval** command to restore the default configuration.

By default, the last listener query interval is 1 second.

Related command: **mld last-listener-query-interval**, **robust-count (MLD view)**and **display mld interface**.

Example # Globally set the last listener query interval to 3 seconds.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] last-listener-query-interval 3
```

max-response-time (MLD view)

Syntax **max-response-time** *interval*

undo max-response-time

View MLD view

Parameter *interval*: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description Use the **max-response-time** command to configure the maximum response delay for general queries globally.

Use the **undo max-response-time** command to restore the default configuration.

By default, the maximum response delay for general queries is 10 seconds.

Related command: **mld max-response-time**, **timer other-querier-present (MLD view)**, and **display mld interface**.

Example # Globally set the maximum response delay for general queries to 8 seconds.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] max-response-time 8
```

mld

Syntax **mld**

undo mld

View System view

Parameter None

Description Use the **mld** command to enter MLD view.

Use the **undo mld** command to remove the configurations done in MLD view.

This command can take effect only after IPv6 multicast routing is enabled on the device.

Related command: **mld enable**, and ***multicast ipv6 routing-enable*** on page 1440.

Example # Enter MLD view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] mld
[Sysname-mld]
```

mld enable

Syntax **mld enable**

undo mld enable

View Interface view

Parameter None

Description Use the **mld enable** command to enable MLD on the current interface.

Use the **undo mld enable** command to disable MLD on the current interface.

By default, MLD is disabled on the current interface.

Note that:

- This command can take effect only after IPv6 multicast routing is enabled on the device.
- Other MLD configurations performed on the interface can take effect only after MLD is enabled on the interface.

Related command: **mld**.

Example # Enable MLD on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld enable
```

mld fast-leave

Syntax **mld fast-leave** [**group-policy** *acl6-number*]

undo mld fast-leave

View Interface view

Parameter *acl6-number*: Number of a basic IPv6 ACL, in the range of 2000 to 2999. If you do not specify any IPv6 ACL number, this command will take effect for all IPv6 multicast groups.

Description Use the **mld fast-leave** command to enable the fast-leave function on the current interface for IPv6 multicast group members.

Use the **undo mld fast-leave** command to disable the fast-leave function on the current interface for IPv6 multicast group members.

By default, the fast-leave function for IPv6 multicast group members is disabled, that is, the MLD querier sends a multicast-address-specific query upon receiving an MLD done message from a host, instead of sending a leave notification directly to the upstream.

Related command: **fast-leave (MLD view)**, **mld last-listener-query-interval**.

Example # Enable the fast-leave function for IPv6 multicast group members on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld fast-leave
```

mld group-policy

Syntax **mld group-policy** *acl6-number* [*version-number*]

undo mld group-policy

View Interface view

Parameter *acl6-number*: Number of a basic or advanced IPv6 ACL, in the range of 2000 to 3999.

version-number: MLD version number, 1 or 2. If you do not specify an MLD version, the configured group filter will apply to MLD reports of both version 1 and version 2.

Description Use the **mld group-policy** command to configure an IPv6 multicast group filter on the current interface to limit access to the IPv6 multicast group.

Use the **undo mld group-policy** command to remove the configured IPv6 multicast group filter.

By default, no IPv6 multicast group filter is configured by default, that is, a host can join any IPv6 multicast group.

When you use an advanced IPv6 ACL as a filter, the source address in the IPv6 ACL is the multicast source address specified in the MLDv2 report message, instead of the source address in the IPv6 message.

Example # Configure an IPv6 ACL so that hosts on the subnet attached to Ethernet 1/0 can join the IPv6 multicast group FF03::101 only.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2005
[Sysname-acl6-basic-2005] rule permit source ff03::101 16
[Sysname-acl6-basic-2005] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld group-policy 2005
```

mld last-listener-query-interval

Syntax **mld last-listener-query-interval** *interval*

undo mld last-listener-query-interval

View Interface view

Parameter *interval*: Last listener query interval in seconds, in the range of 1 to 5.

Description Use the **mld last-listener-query-interval** command to configure the last listener query interval on the current interface.

Use the **undo mld last-listener-query-interval** command to restore the default configuration.

By default, the last listener query interval is 1 second.

Related command: **last-listener-query-interval**, **mld robust-count**, and **display mld interface**.

Example # Set the last listener query interval to 3 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld last-listener-query-interval 3
```

mld max-response-time

Syntax **mld max-response-time** *interval*

undo mld max-response-time

View Interface view

Parameter *interval*: Maximum response delay for MLD general query messages in seconds, in the range of 1 to 25.

Description Use the **mld max-response-time** command to configure the maximum response delay for MLD general query messages on the interface.

Use the **undo mld max-response-time** command to restore the default configuration.

By default, the maximum response delay for MLD general query messages is 10 seconds.

The maximum response delay determines the time which the device takes to detect directly attached group members in the LAN.

Related command: **max-response-time (MLD view)**, **mld timer other-querier-present**, and **display mld interface**.

Example # Set the maximum response delay for MLD general query messages to 8 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld max-response-time 8
```

mld require-router-alert

Syntax **mld require-router-alert**

undo mld require-router-alert

View Interface view

Parameter None

Description Use the **mld require-router-alert** command to configure the interface to discard MLD messages without the Router-Alert option.

Use the **undo mld require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related command: **require-router-alert (MLD view)** and **mld send-router-alert**.

Example # Configure Ethernet1/0 to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld require-router-alert
```

mld robust-count

Syntax **mld robust-count** *robust-value*

undo mld robust-count

View Interface view

Parameter *robust-value*: MLD querier robustness variable, with an effective range of 2 to 5. The MLD robustness variable determines the number of general queries the MLD querier sends on startup and the number of MLD group-specific queries the MLD querier sends upon receiving an MLD done message.

Description Use the **mld robust-count** command to configure the MLD querier robustness variable on the current interface.

Use the **undo mld robust-count** command to restore the system default.

By default, the MLD robustness variable is 2.

Related command: **robust-count (MLD view)**, **mld timer query**, **mld last-listener-query-interval**, **mld timer other-querier-present**, and **display mld interface**.

Example # Set the MLD querier robustness variable to 3 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld robust-count 3
```

mld send-router-alert

Syntax **mld send-router-alert**

undo mld send-router-alert

View Interface view

Parameter None

Description Use the **mld send-router-alert** command to enable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

Use the **undo mld send-router-alert** command to disable insertion of the Router-Alert option into MLD messages to be sent from the current interface.

By default, MLD messages carry the Router-Alert option.

Related command: **send-router-alert (MLD view)** and **mld require-router-alert**.

Example # Disable insertion of the Router-Alert option into MLD messages to be sent from Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo mld send-router-alert
```

mld static-group

Syntax **mld static-group** *ipv6-group-address* [**source** *ipv6-source-address*]

undo mld static-group { **all** | *ipv6-group-address* [**source** *ipv6-source-address*] }

View Interface view

Parameter **all**: Removes all static IPv6 multicast groups that the current interface has joined.

ipv6-group-address: IPv6 multicast group address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16, and FF0y), where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: IPv6 address of the specified multicast source.

Description Use the **mld static-group** command to configure the current interface to be a statically-connected member of the specified IPv6 multicast group.

Use the **undo mld static-group** command to remove the configuration.

By default, an interface is not a statically-connected member of any IPv6 multicast group.

If the IPv6 multicast address is in the SSM multicast address range, and if an IPv6 address is specified for the multicast source, multicast messages carrying the (S,G) entry, namely, the source IPv6 address information, can be sent out of this interface.

Example # Configure Ethernet 1/0 to be a statically-connected member of the multicast group FF03::101.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld static-group ff03::101
```

Configure Ethernet 1/0 to forward multicast data of the multicast source 2001::101 to the multicast group FF04::202.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld static-group ff04::202 source 2001::101
```

mld timer other-querier-present

Syntax **mld timer other-querier-present** *interval*

undo mld timer other-querier-present

View Interface view

Parameter *interval*: MLD other querier present interval in seconds, in the range of 60 to 300.

Description Use the **mld timer other-querier-present** command to configure the MLD other querier present interval on the current interface.

Use the **undo mld timer other-querier-present** command to restore the system default.

By default, the MLD other querier present interval is determined by the following formula:

MLD other querier present interval = [MLD query interval] times [MLD querier robustness variable] plus [maximum response delay for MLD general queries] divided by two.

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the default MLD other querier present interval is 125 x 2 + 10 / 2 = 255 (seconds).

Related command: **timer other-querier-present (MLD view)**, **mld timer query**, **mld robust-count**, **mld max-response-time**, and **display mld interface**.

Example # Set the MLD other querier present interval to 200 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld timer other-querier-present 200
```

mld timer query

Syntax **mld timer query** *interval*

undo mld timer query

View Interface view

Parameter *interval*: query interval, namely the amount of time in seconds between MLD general queries, in the range of 1 to 18,000.

Description Use the **mld timer query** command to configure the query interval on the current interface.

Use the **undo mld timer query** command to restore the default configuration.

By default, the query interval is 125 seconds.

Related command: **mld timer query**, **mld timer other-querier-present**, and **display mld interface**.

Example # Set the query interval to 200 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld timer query 200
```

mld version

Syntax **mld version** *version-number*

undo mld version

View Interface view

Parameter *version-number*: MLD version, 1 or 2.

Description Use the **mld version** command to configure the MLD version on the current interface.

Use the **undo mld version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related command: **mld version**.

Example # Set the MLD version to MLDv2 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mld version 2
```

require-router-alert (MLD view)

Syntax **require-router-alert**

undo require-router-alert

View MLD view

Parameter None

Description Use the **require-router-alert** command to globally configure the device to discard MLD messages without the Router-Alert option.

Use the **undo require-router-alert** command to restore the default configuration.

By default, the device does not check the Router-Alert option, that is, it forwards all received MLD messages to the upper layer protocol for processing.

Related command: **mld require-router-alert** and **send-router-alert (MLD view)**.

Example # Globally configure the device to discard MLD messages without the Router-Alert option.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] require-router-alert
```

reset mld group

Syntax **reset mld group** { **all** | **interface** *interface-type interface-number* { **all** | *ipv6-group-address* [*prefix-length*] [*ipv6-source-address* [*prefix-length*]] } }

View User view

Parameter **all**: Clears all MLD forwarding entries.

interface *interface-type interface-number*: Clears the MLD forwarding entries on the specified interface.

ipv6-group-address: IPv6 address of the specified multicast group, in the range of FFxy::/16, where x and y represent any hexadecimal number ranging from 0 to F.

ipv6-source-address: IPv6 address of the specified multicast source.

prefix-length: Prefix length of the specified multicast source or multicast group. For a multicast source address, this argument has an effective value range of 0 to 128; for a multicast group address, it has an effective value range of 8 to 128. The system default is 128 in both cases.

Description Use the **reset mld group** command to clear MLD forwarding entries.

Note that:

- When you clear MLD forwarding entries on a VLAN interface, the MLD Snooping forwarding entries for this VLAN interface will also be cleared.
- You cannot use this command to clear MLD forwarding entries for static joins.

Related command: **display mld group**.

Example # Clear all MLD forwarding entries on all interfaces.

```
<Sysname> reset mld group all
```

Clear all MLD forwarding entries on Ethernet 1/0.

```
<Sysname> reset mld group interface ethernet 1/0 all
```

Clear all MLD forwarding entries for the IPv6 multicast group FF03::101:10 on Ethernet 1/0.

```
<Sysname> reset mld group interface ethernet 1/0 ff03::101:10
```

Clear all MLD forwarding entries for IPv6 multicast groups in the FF03::101:0/112 range on Ethernet 1/0.

```
<Sysname> reset mld group interface ethernet 1/0 ff03::101:10 112
```

robust-count (MLD view)

Syntax **robust-count** *robust-value*

undo robust-count

View MLD view

Parameter *robust-value*: MLD querier robustness variable, with an effective range of 2 to 5. The MLD robustness variable determines the number of general queries the MLD querier sends on startup and the number of MLD group-specific queries the MLD querier sends upon receiving an MLD done message.

Description Use the **robust-count** command to configure the MLD querier robustness variable globally.

Use the **undo robust-count** command to restore the system default.

By default, the MLD querier robustness variable is 2.

Related command: **mld robust-count**, **last-listener-query-interval**, **timer other-querier-present (MLD view)**, and **display mld interface**.

Example # Set the MLD querier robustness variable to 3 globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] robust-count 3
```

send-router-alert (MLD view)

Syntax **send-router-alert**

undo send-router-alert

View MLD view

Parameter None

Description Use the **send-router-alert** command to globally enable the insertion of the Router-Alert option into MLD messages to be sent.

Use the **undo send-router-alert** command to globally disable the insertion of the Router-Alert option into MLD messages to be sent.

By default, MLD messages carry the Router-Alert option.

Related command: **mld send-router-alert** and **require-router-alert (MLD view)**.

Example # Globally disable insertion of the Router-Alert option into MLD messages to be sent.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] undo send-router-alert
```

timer other-querier-present (MLD view)

Syntax **timer other-querier-present** *interval*

undo timer other-querier-present

View MLD view

Parameter *interval*: MLD other querier present interval in seconds, in the range of 60 to 300.

Description Use the **timer other-querier-present** command to configure the MLD other querier present interval globally.

Use the **undo timer other-querier-present** command to restore the default configuration.

By default, the MLD other querier present interval is determined by the following formula:

MLD other querier present interval = [MLD query interval] times [MLD querier robustness variable] plus [maximum response delay for MLD general queries] divided by two.

By default, the values of the three parameters in the above-mentioned formula are 125, 2, and 10, respectively, so the default MLD other querier present interval is 125 x 2 + 10 / 2 = 255 (seconds).

Related command: **mld timer other-querier-present**, **timer query (MLD view)**, **robust-count (MLD view)**, **max-response-time (MLD view)**, and **display mld interface**.

Example # Set the MLD other querier present interval for non-queriers to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer other-querier-present 200
```

timer query (MLD view)

Syntax **timer query** *interval*

undo timer query

View MLD view

Parameter *interval*: Query interval, namely, amount of time in seconds between MLD general query messages, in the range of 1 to 18,000.

Description Use the **timer query** command to configure the query interval globally.

Use the **undo timer query** command to restore the default configuration.

By default, the query interval is 125 seconds.

Related command: **mld timer query**, **timer other-querier-present (MLD view)**, and **display mld interface**.

Example # Set the query interval to 200 seconds globally.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] timer query 200
```

version (MLD view)

Syntax **version** *version-number*

undo version

View MLD view

Parameter *version-number*: MLD version number, 1 or 2.

Description Use the **version** command to configure the MLD version globally.

Use the **undo version** command to restore the default MLD version.

By default, the MLD version is MLDv1.

Related command: **mld version**.

Example # Globally set the MLD version to MLDv2.

```
<Sysname> system-view
[Sysname] mld
[Sysname-mld] version 2
```

93 IPv6 PIM CONFIGURATION COMMANDS

bsr-policy (IPv6 PIM view)

Syntax **bsr-policy** *acl6-number*

undo bsr-policy

View IPv6 PIM view

Parameter *acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999. When an IPv6 ACL is defined, the **source** keyword in the **rule** command specifies a legal BSR source IPv6 address range.

Description Use the **bsr-policy** command to configure a legal BSR address range to guard against BSR spoofing.

Use the **undo bsr-policy** command to remove the restriction of the BSR address range.

By default, there are no restrictions on the BSR address range, namely all the received BSR messages are regarded to be valid.

Example # Configure a legal BSR address range so that only routers on the segment 2001::2/64 can become the BSR.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2001::2 64
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] bsr-policy 2000
```

c-bsr (IPv6 PIM view)

Syntax **c-bsr** *ipv6-address* [*hash-length* [*priority*]]

undo c-bsr

View IPv6 PIM view

Parameter *ipv6-address*: IPv6 address of the interface that is to act as a C-BSR.

hash-length: Hash mask length for RP selection calculation, in the range of 0 to 128. If you do not include this keyword in your command, the corresponding global setting will be used.

priority: Priority of the C-BSR, in the range of 0 to 255. If you do not include this keyword in your command, the corresponding global setting will be used. A larger value means a higher priority.

Description Use the **c-bsr** command to configure the specified interface a C-BSR.

Use the **undo c-bsr** command to remove the related C-BSR configuration.

No C-BSR is configured by default.

Related command: **pim ipv6 sm**, **c-bsr hash-length (IPv6 PIM view)**, **c-bsr priority (IPv6 PIM view)** and **c-rp (IPv6 PIM view)**.

Example # Configure the interface with an IPv6 address of 1101::1 as a C-BSR.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr 1101::1
```

c-bsr hash-length (IPv6 PIM view)

Syntax **c-bsr hash-length** *hash-length*

undo c-bsr hash-length

View IPv6 PIM view

Parameter *hash-length*: Hash mask length for RP selection calculation, in the range of 0 to 128.

Description Use the **c-bsr hash-length** command to configure the global Hash mask length for RP selection calculation.

Use the **undo c-bsr hash-length** command to restore the system default.

By default, the Hash mask length for RP selection calculation is 126.

Related command: **c-bsr (IPv6 PIM view)** on page 1461.

Example # Set the global Hash mask length for RP selection calculation to 16.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr hash-length 16
```

c-bsr holdtime (IPv6 PIM view)

Syntax **c-bsr holdtime** *interval*

undo c-bsr holdtime

View IPv6 PIM view

Parameter *interval*: Bootstrap timeout in seconds, in the range of 1 to 2,147,483,647.

Description Use the **c-bsr holdtime** command to configure the bootstrap timeout time, namely the length of time for which the C-BSRs wait for a bootstrap message from the BSR.

Use the **undo c-bsr holdtime** command to restore the default setting.

By default, the bootstrap timeout value is determined by this formula: Bootstrap timeout = Bootstrap interval × 2 + 10.

The default bootstrap interval is 60 seconds, so the default bootstrap timeout = 60 × 2 + 10 = 130 (seconds).

Related command: **c-bsr (IPv6 PIM view)** and **c-bsr interval (IPv6 PIM view)**.

Example # Set the bootstrap timeout time to 150 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr holdtime 150
```

c-bsr interval (IPv6 PIM view)

Syntax **c-bsr interval** *interval*

undo c-bsr interval

View IPv6 PIM view

Parameter *interval*: Bootstrap interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **c-bsr interval** command to configure the bootstrap interval, namely the interval at which the BSR sends bootstrap messages.

Use the **undo c-bsr interval** command to restore the default setting.

By default, the bootstrap interval value is determined by this formula: Bootstrap interval = (Bootstrap timeout - 10) / 2.

The default bootstrap timeout is 130 seconds, so the default bootstrap interval = (130 - 10) / 2 = 60 (seconds).

Related command: **c-bsr (IPv6 PIM view)** and **c-bsr holdtime (IPv6 PIM view)**.

Example # Set the bootstrap interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr interval 30
```

c-bsr priority (IPv6 PIM view)

Syntax **c-bsr priority** *priority*

undo c-bsr priority

View IPv6 PIM view

Parameter *priority*: Priority of the C-BSR, in the range of 0 to 255. A larger value means a higher priority.

Description Use the **c-bsr priority** command to configure the global C-BSR priority.

Use the **undo c-bsr priority** command to restore the default setting.

By default, the C-BSR priority is 0.

Related command: **c-bsr (IPv6 PIM view)**.

Example # Set the global C-BSR priority to 5.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-bsr priority 5
```

c-rp (IPv6 PIM view)

Syntax **c-rp** *ipv6-address* [**group-policy** *acl6-number* | **priority** *priority* | **holdtime** *hold-interval* | **advertisement-interval** *adv-interval*] *

undo c-rp *ipv6-address*

View IPv6 PIM view

Parameter *ipv6-address*: IPv6 address of the interface that is to act as a C-RP.

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. This IPv6 ACL defines a range of IPv6 multicast groups the C-RP is going to serve, rather than

defining a filtering rule. Any IPv6 multicast group range that matches the **permit** statement in the ACL will be advertised as an RP served group, while configurations matching other statements like **deny** will not take effect.

priority: Priority of the C-RP, in the range of 0 to 255 and defaulting to 0. A larger value means a lower priority.

hold-interval: C-RP timeout time, in seconds. The effective range is 1 to 65,535. If you do not include provide argument in your command, the corresponding global setting will be used.

adv-interval: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535. If you do not include this argument in your command, the corresponding global setting will be used.

Description Use the **c-rp** command to configure the specified interface as a C-RP.

Use the **undo c-rp** command to remove the related C-RP configuration.

No C-RPs are configured by default.

Note that:

- If you do not specify an IPv6 multicast group range for the C-RP, the C-RP will serve all IPv6 multicast groups.
- If you wish a router to be a C-RP for multiple group ranges, you need to include these group ranges in multiple rules in the IPv6 ACL corresponding to the **group-policy** keyword.
- If you carry out this command repeatedly on the same interface, the last configuration will take effect.

Related command: **c-bsr (IPv6 PIM view)**.

Example # Configure the interface with the IPv6 address of 2001::1 to be a C-RP for IPv6 multicast group FF0E:0:1391::/96, with a priority of 10.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff0e:0:1391:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] c-rp 2001::1 group-policy 2000 priority 10
```

c-rp advertisement-interval (IPv6 PIM view)

Syntax **c-rp advertisement-interval** *interval*

undo c-rp advertisement-interval

View IPv6 PIM view

Parameter *interval*: C-RP-Adv interval in seconds, with an effective range of 1 to 65,535.

Description Use the **c-rp advertisement-interval** command to configure the interval at which C-RP-Adv messages are sent.

Use the **undo c-rp advertisement-interval** command to restore the default setting.

By default, the C-RP-Adv interval is 60 seconds.

Related command: **c-rp (IPv6 PIM view)**.

Example # Set the global C-RP-Adv interval to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp advertisement-interval 30
```

c-rp holdtime (IPv6 PIM view)

Syntax **c-rp holdtime** *interval*

undo c-rp holdtime

View IPv6 PIM view

Parameter *interval*: C-RP timeout in seconds, with an effective range of 1 to 65,535.

Description Use the **c-rp holdtime** command to configure the global C-RP timeout time, namely the length of time the BSR waits for a C-RP-Adv message from C-RPs.

Use the **undo c-rp holdtime** command to restore the default setting.

By default, the C-RP timeout time is 150 seconds.

Because a non-BSR router refreshes its C-RP timeout time through BSR bootstrap messages, to prevent loss of BSR bootstrap messages, make sure that the C-RP timeout time is not smaller than the interval at which the BSR sends bootstrap messages. The recommended C-RP timeout setting is 2.5 times the bootstrap interval or longer.

Related command: **c-rp (IPv6 PIM view)** and **c-bsr interval (IPv6 PIM view)**.

Example # Set the global C-RP timeout time to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] c-rp holdtime 200
```

crp-policy (IPv6 PIM view)

Syntax **crp-policy** *acl6-number*

undo crp-policy

View IPv6 PIM view

Parameter *acl6-number*: Advanced IPv6 ACL number, in the range of 3000 to 3999. When the IPv6 ACL is defined, the **source** keyword in the **rule** command specifies the IPv6 address of a C-RP and the **destination** keyword specifies the IPv6 address range of the IPv6 multicast groups that the C-RP will serve.

Description Use the **crp-policy** command to configure a legal C-RP address range and the range of served IPv6 multicast groups, so as to guard against C-RP spoofing.

Use the **undo crp-policy** command to remove the restrictions in C-RP address ranges and the ranges of served IPv6 multicast groups.

By default, there are no restrictions on C-RP address ranges and the address ranges of served groups, namely all received C-RP messages are assumed to be legal.

Example # Configure a C-RP address range so that only routers in the address range of 2001::2/64 can be C-RPs.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 2001::2 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] crp-policy 3000
```

display pim ipv6 bsr-info

Syntax **display pim ipv6 bsr-info**

View Any view

Parameter None

Description Use the **display pim ipv6 bsr-info** command to view the BSR information in the IPv6 PIM domain and the locally configured C-RP information in effect.

Related command: **c-bsr (IPv6 PIM view)** and **c-rp (IPv6 PIM view)**.

Example # View the BSR information in the IPv6 PIM-SM domain and the locally configured C-RP information in effect.

```
<Sysname> display pim ipv6 bsr-info
Elected BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
     State: Elected
     Uptime: 00:01:10
     Next BSR message scheduled at: 00:00:48
 Candidate BSR Address: 2004::2
     Priority: 0
     Hash mask length: 126
     State: Elected

Candidate RP: 2001::1(LoopBack1)
     Priority: 0
     HoldTime: 130
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
 Candidate RP: 2002::1(Ethernet1/0)
     Priority: 20
     HoldTime: 90
     Advertisement Interval: 50
     Next advertisement scheduled at: 00:00:28
 Candidate RP: 2003::1(Ethernet1/1)
     Priority: 0
     HoldTime: 80
     Advertisement Interval: 60
     Next advertisement scheduled at: 00:00:48
```

Table 354 Description on the fields of the display pim ipv6 bsr-info command

Field	Description
Elected BSR Address	IPv6 address of the elected BSR
Candidate BSR Address	Address of the candidate BSR
Priority	BSR priority
Hash mask length	Hash mask length for RP selection calculation
State	BSR state
Uptime	Length of time since this BSR was elected
Next BSR message scheduled at	Remaining time of this BSR
Candidate RP	Address of the C-RP
Priority	Priority of the C-RP
HoldTime	Timeout time of the C-RP
Advertisement Interval	Interval between C-RP-Adv messages
Next BSR message scheduled at	Remaining time before the C-RP will send the next C-RP-Adv message

display pim ipv6 claimed-route

Syntax **display pim ipv6 claimed-route** [*ipv6-source-address*]

View Any view

Parameter *ipv6-source-address*: Displays the information of the IPv6 unicast route to a particular IPv6 multicast source. If you do not provide this argument, this command will display the information about all IPv6 unicast routes used by IPv6 PIM.

Description Use the **display pim ipv6 claimed-route** command to view the information of IPv6 unicast routes used by IPv6 PIM.

If an (S, G) is marked SPT, this (S, G) entry uses an IPv6 unicast route.

Example # View the information of all IPv6 unicast routes used by IPv6 PIM.

```
<Sysname> display pim ipv6 claimed-route
RPF information about: 2001::2
     RPF interface: Ethernet1/0, RPF neighbor: FE80::A01:100:1
     Referenced prefix/prefix length: 2001::/64
     Referenced route type: igp
     RPF-route selecting rule: preference-preferred
     The (S, G) or (*, G) list dependent on this route entry
     (2001::2, FF03::101)
```

Table 355 Description on the fields of the display pim ipv6 claimed-route command

Field	Description
RPF interface:	RPF interface type and number
RPF neighbor:	IP address of the RPF neighbor
Referenced prefix/prefix length:	Address/mask of the reference route
Referenced route type:	Type of the referenced route
RPF-route selecting rule:	Rule of RPF route selection
The (S,G) or (*,G) list dependent on this route entry	(S,G) or (*, G) entries using this route

display pim ipv6 control-message counters

Syntax **display pim ipv6 control-message counters** [**message-type** { **probe** | **register** | **register-stop** } | [**interface** *interface-type interface-number* | **message-type** { **assert** | **bsr** | **crp** | **graf**t | **graft-ack** | **hello** | **join-prune** | **state-refresh** }] *]

View Any view

Parameter **probe**: Displays the number of null register messages.

register: Displays the number of register messages.

register-stop: Displays the number of register-stop messages.

interface *interface-type interface-number*: Displays the number of IPv6 PIM control messages on the specified interface.

assert: Displays the number of assert messages.

bsr: Displays the number of bootstrap messages.

crp: Displays the number of C-RP-Adv messages.

graft: Displays the number of graft messages.

graft-ack: Displays the number of graft-ack messages.

hello: Displays the number of hello messages.

join-prune: Displays the number of join/prune messages.

state-refresh: Displays the number of state refresh messages.

Description Use the **display pim ipv6 control-message counters** command to view the statistics information of IPv6 PIM control messages.

Example # View the statistics information of all types of IPv6 PIM control messages on all interfaces.

```
<Sysname> display pim ipv6 control-message counters
PIM global control-message counters:
                  Received      Sent            Invalid
Register            20          37          2
Register-Stop       25          20          1
Probe               10          5           0

PIM control-message counters for interface: Ethernet1/0
                    Received      Sent            Invalid
Assert          10          5           0
Graft               20          37          2
Graft-Ack           25          20          1
Hello               1232            453         0
Join/Prune      15          30          21
State-Refresh       8           7           1
BSR             3243            589         1
C-RP                53          32          0
```

Table 356 Description on the fields of the display pim ipv6 control-message counters command

Field	Description
Received	Number of messages received
Sent	Number of messages sent
Invalid	Number of invalid messages
Register	Register messages
Register-Stop	Register-stop messages
Probe	Null register messages
Assert	Assert messages
Graft	Graft messages
Graft-Ack	Graft-ack messages
Hello	Hello messages
Join/Prune	Join/prune messages
State Refresh	State refresh messages
BSR	Bootstrap messages

Table 356 Description on the fields of the display pim ipv6 control-message counters command

Field	Description
C-RP	C-RP-Adv messages

display pim ipv6 grafts

Syntax **display pim ipv6 grafts**

View Any view

Parameter None

Description Use the **display pim ipv6 grafts** command to view the information about unacknowledged graft messages.

Example # View the information about unacknowledged graft messages.

```
<Sysname> display pim ipv6 grafts
Source              Group              Age           RetransmitIn
1004::2             ff03::101          00:00:24      00:00:02
```

Table 357 Description on the fields of the display pim ipv6 grafts command

Field	Description
Source	IPv6 multicast source address in the graft message
Group	IPv6 multicast group address in the graft message
Age	Time in which the graft message will get aged out, in hours:minutes:seconds
RetransmitIn	Time in which the graft message will be retransmitted, in hours:minutes:seconds

display pim ipv6 interface

Syntax **display pim ipv6 interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *interface-type interface-number*: Displays the IPv6 PIM information on a particular interface.

verbose: Displays the detailed PIM information.

Description Use the **display pim ipv6 interface** command to view the IPv6 PIM information on the specified interface or all interfaces.

Example # View the detailed IPv6 PIM information on Ethernet 1/0.

```
<Sysname> display pim ipv6 interface ethernet 1/0 verbose
Interface; Ethernet1/0, FE80::200:5EFF:FE04:8700
     PIM version: 2
     PIM mode: Sparse
     PIM DR: FE80::200:AFF:FE01:101
     PIM DR Priority (configured): 1
     PIM neighbor count: 1
     PIM hello interval: 30 s
     PIM LAN delay (negotiated): 500 ms
     PIM LAN delay (configured): 500 ms
     PIM override interval (negotiated): 2500 ms
     PIM override interval (configured): 2500 ms
     PIM neighbor tracking (negotiated): disabled
     PIM neighbor tracking (configured): disabled
     PIM generation ID: 0xF5712241
     PIM require generation ID: disabled
     PIM hello hold interval: 105 s
     PIM assert hold interval: 180 s
     PIM triggered hello delay: 5 s
     PIM J/P interval: 60 s
     PIM J/P hold interval: 210 s
     PIM BSR domain border: disabled
     Number of routers on network not using DR priority: 0
     Number of routers on network not using LAN delay: 0
     Number of routers on network not using neighbor tracking: 2
```

Table 358 Description on the fields of the display pim ipv6 interface command

Field	Description
Interface	Interface name and its IPv6 address
PIM version	IPv6 PIM version
PIM mode	IPv6 PIM mode, dense or sparse
PIM DR	IPv6 address of the DR
PIM DR Priority (configured)	Priority for DR election
PIM neighbor count	Total number of IPv6 PIM neighbors
PIM hello interval	Interval between IPv6 PIM hello messages
PIM LAN delay (negotiated)	Negotiated prune delay
PIM LAN delay (configured)	Configured prune delay
PIM override interval (negotiated)	Negotiated prune override interval
PIM override interval (configured)	Configured prune override interval
PIM neighbor tracking (negotiated)	Negotiated neighbor tracking status (enabled/disabled)
PIM neighbor tracking (configured)	Configured neighbor tracking status (enabled/disabled)
PIM generation ID	Generation_ID value
PIM require generation ID	Rejection of Hello messages without Generation_ID (enabled/disabled)
PIM hello hold interval	IPv6 PIM neighbor timeout time
PIM assert hold interval	Assert timeout time
PIM triggered hello delay	Maximum delay of sending hello messages
PIM J/P interval	Join/prune interval

Table 358 Description on the fields of the display pim ipv6 interface command

Field	Description
PIM J/P hold interval	Join/prune timeout time
PIM BSR domain border	BSR administrative scoping status (enabled/disabled)
Number of routers on network not using DR priority	Number of routers not using the DR priority field on the subnet where the interface resides
Number of routers on network not using LAN delay	Number of routers not using the LAN delay field on the subnet where the interface resides
Number of routers on network not using neighbor tracking	Number of routers not using neighbor tracking on the subnet where the interface resides

display pim ipv6 join-prune

Syntax **display pim ipv6 join-prune mode** { **sm** [**flags** *flag-value*] | **ssm** } [**interface** *interface-type interface-number* | **neighbor** *ipv6-neighbor-address*] * [**verbose**]

View Any view

Parameter **mode**: Displays the information of join/prune messages to send in the specified IPv6 PIM mode. IPv6 PIM modes include **sm** and **ssm**, which represent IPv6 PIM-SM and IPv6 PIM-SSM respectively.

flags *flag-value*: Specifies to display IPv6 PIM routing entries containing the specified flag(s).Values and meanings of *flag-value* are as follows:

- **rpt**: Specifies routing entries on the RPT.
- **spt**: Specifies routing entries on the SPT.
- **wc**: Specifies wildcard routing entries.

interface-type interface-number: Displays the information of join/prune messages to send on the specified interface.

ipv6-neighbor-address: Displays the information of join/prune messages to send to the specified IPv6 PIM neighbor.

verbose: Displays the detailed information of join/prune messages to send.

Description Use the **display pim join-prune** command to view the information about the join/prune messages to send.

Example # View the information of join/prune messages to send in the IPv6 PIM-SM mode.

```
<Sysname> display pim ipv6 join-prune mode sm

 Expiry Time: 50 sec
 Upstream nbr: FE80::2E0:FCFF:FE03:1004 (Ethernet1/1)
 1 (*, G) join(s), 0 (S, G) join(s), 1 (S, G, rpt) prune(s)
```

```
------------------------------------------------------------------------
 Total (*, G) join(s): 1, (S, G) join(s): 0, (S, G, rpt) prune(s): 1
```

Table 359 Description on the fields of the display pim join-prune command

Field	Description
Expiry Time:	Expiry time of sending join/prune messages
Upstream nbr:	IPv6 address of the upstream IPv6 PIM neighbor and the interface connecting to it
(*, G) join(s)	Number of (*, G) joins to send
(S, G) join(s)	Number of (S, G) joins to send
(S, G, rpt) prune(s)	Number of (S, G, rpt) prunes

display pim ipv6 neighbor

Syntax **display pim ipv6 neighbor** [**interface** *interface-type interface-number* | *ipv6-neighbor-address* | **verbose**] *

View Any view

Parameter *interface-type interface-number*: Displays the IPv6 PIM neighbor information on a particular interface.

ipv6-neighbor-address: Displays the information of a particular IPv6 PIM neighbor.

verbose: Displays the detailed IPv6 PIM neighbor information.

Description Use the **display pim ipv6 neighbor** command to view the IPv6 PIM neighbor information.

Example # View the information of all IPv6 PIM neighbors.

```
<Sysname> display pim neighbor
 Total Number of Neighbors = 2

 Neighbor           Interface          Uptime   Expires  Dr-Priority
 FE80::A01:101:1    Eth1/0             02:50:49 00:01:31 1
 FE80::A01:102:1    Eth1/1             02:49:39 00:01:42 1
```

Table 360 Description on the fields of the display pim ipv6 neighbor command

Field	Description
Total Number of Neighbors	Total number of IPv6 PIM neighbors
Neighbor	IPv6 address of the PIM neighbor
Interface	Interface connecting the IPv6 PIM neighbor
Uptime	Length of time since the IPv6 PIM neighbor was discovered
Expires	Remaining time of the IPv6 PIM neighbor
Dr-Priority	Designated router priority

display pim ipv6 routing-table

Syntax **display pim ipv6 routing-table** [*ipv6-group-address* [*prefix-length*] | *ipv6-source-address* [*prefix-length*] | **incoming-interface** [*interface-type interface-number* | **register**] | **outgoing-interface** { **include** | **exclude** | **match** } { *interface-type interface-number* | **register** } | **mode** *mode-type* | **flags** *flag-value* | **fsm**] *

View Any view

Parameter *ipv6-group-address*: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16, where x and y represent any hexadecimal number between 0 and F, inclusive.

ipv6-source-address: Specifies an IPv6 multicast source by its IPv6 address.

prefix-length: Prefix length of the IPv6 multicast group/source address. For an IPv6 multicast group address, the effective range is 8 to 128 and the default value is 128; for an IPv6 multicast source address, the effective range is 0 to 128 and the default value is 128.

incoming-interface: Displays routing entries that contain the specified interface as the incoming interface.

interface-type interface-number: Specifies an interface by its type and number.

register: Specifies the register interface. This keyword is valid only if *mode-type* is not specified or is **sm**

outgoing-interface: Displays routing entries that contain the specified interface as the outgoing interface.

include: Displays routing entries of which the outgoing interface list includes the specified interface.

exclude: Displays routing entries of which the outgoing interface list excludes the specified interface.

match: Displays routing entries of which the outgoing interface list includes only the specified interface.

mode *mode-type*: Specifies an IPv6 PIM mode, where *mode-type* can have the following values:

- **dm**: Specifies IPv6 PIM-DM.
- **sm**: Specifies IPv6 PIM-SM.
- **ssm**: Specifies IPv6 PIM-SSM.

flags *flag-value*: Displays IPv6 PIM routing entries containing the specified flag(s). The values of *flag-value* and their meanings are as follows:

- **act**: Specifies IPv6 multicast routing entries to which actual data has arrived.

- **del**: Specifies IPv6 multicast routing entries scheduled to be deleted.
- **exprune**: Specifies multicast routing entries containing outgoing interfaces pruned by other IPv6 multicast routing protocols.
- **ext**: Specifies IPv6 routing entries containing outgoing interfaces contributed by other IPv6 multicast routing protocols.
- **loc**: Specifies IPv6 multicast routing entries on routers directly connecting to the same subnet with the IPv6 multicast source.
- **niif**: Specifies IPv6 multicast routing entries containing unknown incoming interfaces.
- **nonbr**: Specifies routing entries with IPv6 PIM neighbor searching failure.
- **rpt**: Specifies routing entries on RPT branches where (S, G) prunes have been sent to the RP.
- **spt**: Specifies routing entries on the SPT.
- **swt**: Specifies routing entries in the process of RPT-to-SPT switchover.
- **wc**: Specifies wildcard routing entries.

fsm: Displays the detailed information of the finite state machine (FSM).

Description Use the **display pim ipv6 routing-table** command to view IPv6 PIM routing table information.

Related command: **display multicast ipv6 routing-table** on page 1434.

Example # View the content of the IPv6 PIM routing table.

```
<Sysname> display pim ipv6 routing-table
 Total 0 (*, G) entry; 1 (S, G) entry

(2001::2, FFE3::101)
     Protocol: pim-dm, Flag:
     UpTime: 00:04:24
     Upstream interface: Ethernet1/0
         Upstream neighbor: FE80::A01:100:1
         RPF prime neighbor: FE80::A01:100:1
     Downstream interface(s) information:
     Total number of downstreams: 1
         1: Ethernet1/1
             Protocol: pim-dm, UpTime: 00:04:24, Expires: 00:02:47
```

Table 361 Description on the fields of the display pim ipv6 routing-table command

Field	Description
Total 0 (*, G) entry; 1 (S, G) entry	Number of (S,G) and (*, G) entries in the IPv6 PIM routing table
(2001::2, FFE3::101)	An (S,G) entry in the IPv6 PIM routing table
Protocol	IPv6 PIM mode, IPv6 PIM-SM or IPv6 PIM-DM
Flag	Flag of the (S, G) or (*, G) entry in the IPv6 PIM routing table
Uptime	Length of time since the (S, G) or (*, G) entry was installed
Upstream interface	Upstream (incoming) interface of the (S, G) or (*, G) entry
Upstream neighbor	Upstream neighbor of the (S, G) or (*, G) entry

Table 361 Description on the fields of the display pim ipv6 routing-table command

Field	Description
RPF prime neighbor	RPF neighbor of the (S, G) or (*, G) entry ■ For a (*, G) entry, if this router is the RP, the RPF neighbor of this (*, G) entry is NULL. ■ For a (S, G) entry, if this router directly connects to the IPv6 multicast source, the RPF neighbor of this (S, G) entry is NULL.
Downstream interface(s) information	Information of the downstream interface(s), including: ■ Number of downstream interfaces ■ Downstream interface name ■ Protocol type configured on the downstream interface ■ Uptime of the downstream interface(s) ■ Expiry time of the downstream interface(s)

display pim ipv6 rp-info

Syntax **display pim ipv6 rp-info** [*ipv6-group-address*]

View Any view

Parameter *ipv6-group-address*: Specifies an IPv6 multicast group by its address, in the range of FFxy::/16 (excluding FFx0::/16, FFx1::/16, FFx2::/16 and FF0y::), where x and y represent any hexadecimal number between 0 and F, inclusive. If you do not provide a group address, this command will display the RP information corresponding to all IPv6 multicast groups.

Description Use the **display pim ipv6 rp-info** command to view the RP information.

Note that:

- The RP information includes the information of RPs dynamically found by the BSR mechanism and static RPs.
- Because a non-BSR router refreshes its local RP-Set only based on the received BSR bootstrap messages, the system does not delete an RP even if its expiry time is 0. Instead, the system waits for the next bootstrap message from the BSR: if the bootstrap message does not contain information of the RP, the system will delete it.

Example # View the RP information corresponding to the IPv6 multicast group FF0E::101.

```
<Sysname> display pim ipv6 rp-info ff0e::101
PIM-SM BSR RP information:
 prefix/prefix length: FF0E::101/64
     RP: 2004::2
     Priority: 0
     HoldTime: 130
     Uptime: 00:05:19
     Expires: 00:02:11
```

Table 362 Description on the fields of the display pim ipv6 rp-info command

Field	Description
prefix/prefix length	The IPv6 multicast group served by the RP
RP	IPv6 address of the RP
Priority	RP priority
HoldTime	Timeout time of the RP
Uptime	Length of time since the RP was elected
Expires	Remaining time of the RP

embedded-rp

Syntax **embedded-rp** [*acl6-number*]

undo embedded-rp [*acl6-number*]

View IPv6 PIM view

Parameter *acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999.

Description Use the **embedded-rp** command to enable embedded RP.

Use the **undo embedded-rp** command to disable embedded RP or restore the default configuration.

By default, any IPv6 multicast group in the default embedded RP address ranges can use the embedded RP function.

The default embedded RP address ranges are FF7x::/12 and FFFx::/12, where x represents any legal scope.

For details about the scope field, refer to "MPLS Basics Configuration Commands" on page 1513.

Note that:

- When you use the **embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be enabled for all the IPv6 multicast groups in the default embedded RP address scopes; if you specify *acl6-number*, the embedded RP feature will be enabled for only those IPv6 multicast groups that are within the default embedded RP address scopes and pass the ACL check.
- When you use the **undo embedded-rp** command without specifying *acl6-number*, the embedded RP feature will be disabled for all the IPv6 multicast groups; if you specify *acl6-number*, this command will restore the system default.

Example # Enable embedded RP for the IPv6 multicast groups in the range of FF7E:140:20::101/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff7e:140:20::101 64
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] embedded-rp 2000
```

hello-option dr-priority (IPv6 PIM view)

Syntax **hello-option dr-priority** *priority*

undo hello-option dr-priority

View IPv6 PIM view

Parameter *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description Use the **hello-option dr-priority** command to configure the global value of the router priority for DR election.

Use the **undo hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

Related command: **pim ipv6 hello-option dr-priority**.

Example # Set the router priority for DR election to 3.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option dr-priority 3
```

hello-option holdtime (IPv6 PIM view)

Syntax **hello-option holdtime** *interval*

undo hello-option holdtime

View IPv6 PIM view

Parameter *interval*: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **hello-option holdtime** command to configure the IPv6 PIM neighbor timeout time.

Use the **undo hello-option holdtime** command to restore the default setting.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related command: **pim ipv6 hello-option holdtime**.

Example # Set the IPv6 PIM neighbor timeout time to 120 seconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option holdtime 120
```

hello-option lan-delay (IPv6 PIM view)

Syntax **hello-option lan-delay** *interval*

undo hello-option lan-delay

View IPv6 PIM view

Parameter *interval*: Prune delay in milliseconds, with an effective range of 1 to 32,767.

Description Use the **hello-option lan-delay** command to configure the global value of prune delay time, namely the length of time the device must wait upon receiving a prune message from downstream before taking the prune action. Within this period of time, if the device receives a prune override message from that downstream device, the prune action will be cancelled.

Use the **undo hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

Related command: **hello-option override-interval (IPv6 PIM view)**, **pim ipv6 hello-option override-interval** and **pim ipv6 hello-option lan-delay**.

Example # Set the prune delay to 200 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option lan-delay 200
```

hello-option neighbor-tracking (IPv6 PIM view)

Syntax **hello-option neighbor-tracking**

undo hello-option neighbor-tracking

View IPv6 PIM view

Parameter None

Description Use the **hello-option neighbor-tracking** command to globally disable join suppression, namely enable neighbor tracking.

Use the **undo hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related command: **pim ipv6 hello-option neighbor-tracking**.

Example # Disable join suppression globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option neighbor-tracking
```

hello-option override-interval (IPv6 PIM view)

Syntax **hello-option override-interval** *interval*

undo hello-option override-interval

View IPv6 PIM view

Parameter *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description Use the **hello-option override-interval** command to configure the global value of the prune override interval.

Use the **undo hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

Related command: **hello-option lan-delay (IPv6 PIM view)**, **pim ipv6 hello-option lan-delay** and **pim ipv6 hello-option override-interval**.

Example # Set the prune override interval to 2,000 milliseconds globally.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] hello-option override-interval 2000
```

holdtime assert (IPv6 PIM view)

Syntax **holdtime assert** *interval*

undo holdtime assert

View IPv6 PIM view

Parameter *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description Use the **holdtime assert** command to configure the global value of the assert timeout time.

Use the **undo holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

Related command: **holdtime join-prune (IPv6 PIM view)**, **pim ipv6 holdtime join-prune** and **pim ipv6 holdtime assert**.

Example # Set the global value of the assert timeout time to 100 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime assert 100
```

holdtime join-prune (IPv6 PIM view)

Syntax **holdtime join-prune** *interval*

undo holdtime join-prune

View IPv6 PIM view

Parameter *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **holdtime join-prune** command to configure the global value of the join/prune timeout time.

Use the **undo holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

Related command: **holdtime assert (IPv6 PIM view)**, **pim ipv6 holdtime assert** and **pim ipv6 holdtime join-prune**.

Example # Set the global value of the join/prune timeout time to 280 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] holdtime join-prune 280
```

jp-pkt-size (IPv6 PIM view)

Syntax **jp-pkt-size** *packet-size*

undo jp-pkt-size

View IPv6 PIM view

Parameter *packet-size*: Maximum size of join/prune messages in bytes, with an effective range of 100 to 64000.

Description Use the **jp-pkt-size** command to configure the maximum size of join/prune messages.

Use the **undo jp-pkt-size** command to restore the default setting.

By default, the maximum size of join/prune messages is 8,100 bytes.

Related command: **jp-queue-size (IPv6 PIM view)**.

Example # Set the maximum size of join/prune messages to 1,500 bytes.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-pkt-size 1500
```

jp-queue-size (IPv6 PIM view)

Syntax **jp-queue-size** *queue-size*

undo jp-queue-size

View IPv6 PIM view

Parameter *queue-size*: Maximum number of (S, G) entries in a join/prune message, in the range of 1 to 4,096.

Description Use the **jp-queue-size** command to configure the maximum number of (S, G) entries in a join/prune message.

Use the **undo jp-queue-size** command to restore the default setting.

By default, a join/prune messages contains a maximum of 1,020 (S, G) entries.

When you use this command, take the following into account:

- The size of the forwarding table. In a network that does not support packet fragmentation, if you configure a large queue-size, a join/prune message may contain a large number of groups, causing the message length to exceed the

MTU of the network. As a result, the products that do not support fragmentation will drop the join/prune message.

- The (S, G) join/prune state hold time on the upstream device. If you configure a small queue size, the outgoing interface of the corresponding entry may have been pruned due to timeout before the last join/prune message in a queue reaches the upstream device.

Related commands: **jp-pkt-size (IPv6 PIM view)**, **holdtime join-prune (IPv6 PIM view)**, **pim ipv6 holdtime join-prune**.

Example # Configure a join/prune messages to contain a maximum of 2,000 (S, G) entries.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] jp-queue-size 2000
```

pim ipv6

Syntax **pim ipv6**

undo pim ipv6

View System view

Parameter None

Description Use the **pim ipv6** command to enter IPv6 PIM view.

Use the **undo pim ipv6** command to remove all configurations performed in IPv6 PIM view.

IPv6 multicast must be enabled on the device before this command can take effect.

Related command: **multicast ipv6 routing-enable** on page 1440.

Example # Enable IPv6 multicast routing and enter IPv6 PIM view.

```
<Sysname> system-view
[Sysname] multicast ipv6 routing-enable
[Sysname] pim ipv6
[Sysname-pim6]
```

pim ipv6 bsr-boundary

Syntax **pim ipv6 bsr-boundary**

undo pim ipv6 bsr-boundary

View Interface view

Parameter None

Description Use the **pim ipv6 bsr-boundary** command to configure a BSR admin-scope region boundary on the current interface.

Use the **undo pim ipv6 bsr-boundary** command to remove the configured BSR admin-scope region boundary.

By default, no BSR admin-scope region boundary is configured.

Related command: **c-bsr (IPv6 PIM view)**, **multicast ipv6 boundary** on page 1436.

Example # Configure Ethernet 1/0 to be the boundary of the BSR admin-scope region.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 bsr-boundary
```

pim ipv6 dm

Syntax **pim ipv6 dm**

undo pim ipv6 dm

View Interface view

Parameter None

Description Use the **pim ipv6 dm** command to enable IPv6 PIM-DM.

Use the **undo pim ipv6 dm** command to disable IPv6 PIM-DM.

By default, IPv6 PIM-DM is disabled.

Note that IPv6 PIM-DM cannot be used for IPv6 multicast groups in the IPv6 SSM group range.

Related commands: **pim ipv6 sm**, **ssm-policy (IPv6 PIM view)**.

Example # Enable IPv6 PIM-DM on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 dm
```

pim ipv6 hello-option dr-priority

Syntax **pim ipv6 hello-option dr-priority** *priority*

undo pim ipv6 hello-option dr-priority

View Interface view

Parameter *priority*: Router priority for DR election, in the range of 0 to 4294967295. A larger value of this argument means a higher priority.

Description Use the **pim ipv6 hello-option dr-priority** command to configure the router priority for DR election on the current interface.

Use the **undo pim ipv6 hello-option dr-priority** command to restore the default setting.

By default, the router priority for DR election is 1.

Related command: **hello-option dr-priority (IPv6 PIM view)**.

Example # Set the router priority for DR election to 3 on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 hello-option dr-priority 3
```

pim ipv6 hello-option holdtime

Syntax **pim ipv6 hello-option holdtime** *interval*

undo pim ipv6 hello-option holdtime

View Interface view

Parameter *interval*: IPv6 PIM neighbor timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **pim ipv6 hello-option holdtime** command to configure the PIM neighbor timeout time on the current interface.

Use the **undo pim ipv6 hello-option holdtime** command to restore the default setting.

By default, the IPv6 PIM neighbor timeout time is 105 seconds.

Related command: **hello-option holdtime (IPv6 PIM view)**.

Example # Set the IPv6 PIM neighbor timeout time to 120 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 hello-option holdtime 120
```

pim ipv6 hello-option lan-delay

Syntax **pim ipv6 hello-option lan-delay** *interval*

undo pim ipv6 hello-option lan-delay

View Interface view

Parameter *interval*: Prune delay in milliseconds, with an effective range of 1 to 32,767.

Description Use the **pim ipv6 hello-option lan-delay** command to configure the prune delay time on the current interface.

Use the **undo pim ipv6 hello-option lan-delay** command to restore the default setting.

By default, the prune delay to 500 milliseconds.

Related command: **pim ipv6 hello-option override-interval**, **hello-option override-interval (IPv6 PIM view)**, and **hello-option lan-delay (IPv6 PIM view)**.

Example # Set the prune delay time to 200 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 hello-option lan-delay 200
```

pim ipv6 hello-option neighbor-tracking

Syntax **pim ipv6 hello-option neighbor-tracking**

undo pim ipv6 hello-option neighbor-tracking

View Interface view

Parameter None

Description Use the **pim ipv6 hello-option neighbor-tracking** command to disable join suppression, namely enable neighbor tracking, on the current interface.

Use the **undo pim ipv6 hello-option neighbor-tracking** command to enable join suppression.

By default, join suppression is enabled, namely neighbor tracking is disabled.

Related command: **hello-option neighbor-tracking (IPv6 PIM view)**.

Example # Disable join suppression on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 hello-option neighbor-tracking
```

pim ipv6 hello-option override-interval

Syntax **pim ipv6 hello-option override-interval** *interval*

undo pim ipv6 hello-option override-interval

View Interface view

Parameter *interval*: Prune override interval in milliseconds, with an effective range of 1 to 65,535.

Description Use the **pim ipv6 hello-option override-interval** command to configure the prune override interval on the current interface.

Use the **undo pim ipv6 hello-option override-interval** command to restore the default setting.

By default, the prune override interval is 2,500 milliseconds.

Related command: **pim ipv6 hello-option lan-delay**, **hello-option lan-delay (IPv6 PIM view)**, and **hello-option override-interval (IPv6 PIM view)**.

Example # Set the prune override interval to 2,000 milliseconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 hello-option override-interval 2000
```

pim ipv6 holdtime assert

Syntax **pim ipv6 holdtime assert** *interval*

undo pim ipv6 holdtime assert

View Interface view

Parameter *interval*: Assert timeout time in seconds, with an effective range of 7 to 2,147,483,647.

Description Use the **pim ipv6 holdtime assert** command to configure the assert timeout time on the current interface.

Use the **undo pim ipv6 holdtime assert** command to restore the default setting.

By default, the assert timeout time is 180 seconds.

Related command: **holdtime join-prune (IPv6 PIM view)**, **pim ipv6 holdtime join-prune**, and **holdtime assert (IPv6 PIM view)**.

Example # Set the assert timeout time to 100 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 holdtime assert 100
```

pim ipv6 holdtime join-prune

Syntax **pim ipv6 holdtime join-prune** *interval*

undo pim ipv6 holdtime join-prune

View Interface view

Parameter *interval*: Join/prune timeout time in seconds, with an effective range of 1 to 65,535.

Description Use the **pim ipv6 holdtime join-prune** command to configure the join/prune timeout time on the interface.

Use the **undo pim ipv6 holdtime join-prune** command to restore the default setting.

By default, the join/prune timeout time is 210 seconds.

Related command: **holdtime assert (IPv6 PIM view)**, **pim ipv6 holdtime assert**, and **holdtime join-prune (IPv6 PIM view)**.

Example # Set the join/prune timeout time to 280 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 holdtime join-prune 280
```

pim ipv6 require-genid

Syntax **pim ipv6 require-genid**

undo pim ipv6 require-genid

View Interface view

Parameter None

Description Use the **pim ipv6 require-genid** command enable rejection of hello messages without Generation_ID.

Use the **undo pim ipv6 require-genid** command to restore the default configuration.

By default, hello messages without Generation_ID are accepted.

Example # Enable Ethernet 1/0 to reject hello messages without Generation_ID.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 require-genid
```

pim ipv6 sm

Syntax **pim ipv6 sm**

undo pim ipv6 sm

View Interface view

Parameter None

Description Use the **pim ipv6 sm** command to enable IPv6 PIM-SM.

Use the **undo pim ipv6 sm** command to disable IPv6 PIM-SM.

By default, IPv6 PIM-SM is disabled.

Related command: **pim ipv6 dm**.

Example # Enable IPv6 PIM-SM on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 sm
```

pim ipv6 state-refresh-capable

Syntax **pim ipv6 state-refresh-capable**

undo pim ipv6 state-refresh-capable

View Interface view

Parameter None

Description Use the **pim ipv6 state-refresh-capable** command to enable the state fresh feature on the interface.

Use the **undo pim ipv6 state-refresh-capable** command to disable the state fresh feature.

By default, the state refresh feature is enabled.

Related command: **state-refresh-interval (IPv6 PIM view)**, **state-refresh-rate-limit (IPv6 PIM view)**, and **state-refresh-hoplimit**.

Example # Disable state refresh on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo pim ipv6 state-refresh-capable
```

pim ipv6 timer graft-retry

Syntax **pim ipv6 timer graft-retry** *interval*

undo pim ipv6 timer graft-retry

View Interface view

Parameter *interval*: Graft retry period in seconds, with an effective range of 1 to 65,535.

Description Use the **pim ipv6 timer graft-retry** command to configure the graft retry period.

Use the **undo pim ipv6 timer graft-retry** command to restore the default setting.

By default, the graft retry period is 3 seconds.

Example # Set the graft retry period to 80 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 timer graft-retry 80
```

pim ipv6 timer hello

Syntax **pim ipv6 timer hello** *interval*

undo pim ipv6 timer hello

View Interface view

Parameter *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **pim ipv6 timer hello** command to configure on the current interface the interval at which hello messages are sent.

Use the **undo pim ipv6 timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

Related command: **timer hello (IPv6 PIM view)**.

Example # Set the hello interval to 40 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 timer hello 40
```

pim ipv6 timer join-prune

Syntax **pim ipv6 timer join-prune** *interval*

undo pim ipv6 timer join-prune

View Interface view

Parameter *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **pim ipv6 timer join-prune** command to configure on the current interface the interval at which join/prune messages are sent.

Use the **undo pim ipv6 timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

Related command: **timer join-prune (IPv6 PIM view)**.

Example # Set the join/prune interval to 80 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 timer join-prune 80
```

pim ipv6 triggered-hello-delay

Syntax **pim ipv6 triggered-hello-delay** *interval*

undo pim ipv6 trigged-hello-delay

View Interface view

Parameter *interval*: Maximum delay in seconds between hello messages, with an effective range of 1 to 5.

Description Use the **pim ipv6 triggered-hello-delay** command to configure the maximum delay between hello messages.

Use the **undo pim ipv6 triggered-hello-delay** command to restore the default setting.

By default, the maximum delay between hello messages is 5 seconds.

Example # Set the maximum delay between hello messages to 3 seconds on Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] pim ipv6 trigged-hello-delay 3
```

probe-interval (IPv6 PIM view)

Syntax **probe-interval** *interval*

undo probe-interval

View IPv6 PIM view

Parameter *interval*: Register probe time in seconds, with an effective range of 1 to 3,600.

Description Use the **probe-interval** command to configure the register probe time.

Use the **undo probe-interval** command to restore the default setting.

By default, the register probe time is 5 seconds.

Related command: **register-suppression-timeout (IPv6 PIM view)**.

Example # Set the probe time to 6 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] probe-interval 6
```

register-policy (IPv6 PIM view)

Syntax **register-policy** *acl6-number*

undo register-policy

View IPv6 PIM view

Parameter *acl6-number*: Advanced IPv6 ACL number, in the range of 3000 to 3999. Only register messages that match the **permit** statement of the IPv6 ACL can be accepted by the RP.

Description Use the **register-policy** command to configure an IPv6 ACL rule to filter register messages.

Use the **undo register-policy** command to remove the configured register filtering rule.

By default, no register filtering rule is configured.

Related command: **register-suppression-timeout (IPv6 PIM view)**.

Example # Configure a register filtering policy on the RP so that only IPv6 multicast sources on the subnet 3:1::/64 can send IPv6 multicast data to the IPv6 multicast groups on the subnet FF0E:13::/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit ipv6 source 3:1:: 64 destination
 ff0e:13:: 64
[Sysname-acl6-adv-3000] quit
[Sysname] pim ipv6
[Sysname-pim6] register-policy 3000
```

register-suppression-timeout (IPv6 PIM view)

Syntax **register-suppression-timeout** *interval*

undo register-suppression-timeout

View IPv6 PIM view

Parameter *interval*: Register suppression timeout in seconds, in the range of 1 to 3,600.

Description Use the **register-suppression-timeout** command to configure the register suppression timeout time.

Use the **undo register-suppression-timeout** command to restore the default setting.

By default, the register suppression timeout time is 60 seconds.

Related command: **probe-interval (IPv6 PIM view)** and **register-policy (IPv6 PIM view)**.

Example # Set the register suppression timeout time to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-suppression-timeout 70
```

register-whole-checksum (IPv6 PIM view)

Syntax **register-whole-checksum**

undo register-whole-checksum

View IPv6 PIM view

Parameter None

Description Use the **register-whole-checksum** command to configure the router to calculate the checksum based on the entire register message.

Use the **undo register-whole-checksum** command to restore the default configuration.

By default, the checksum is calculated based only on the header in the register message.

Related command: **register-policy (IPv6 PIM view)** and **register-suppression-timeout (IPv6 PIM view)**.

Example # Configure the router to calculate the checksum based on the entire register message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] register-whole-checksum
```

reset pim ipv6 control-message counters

Syntax **reset pim ipv6 control-message counters** [**interface** *interface-type interface-number*]

View User view

Parameter *interface-type interface-number*: Specifies to reset the IPv6 PIM control message counter on a particular interface. If no interface is specified, this command will clear the statistics information about IPv6 PIM control messages on all interfaces.

Description Use the **reset pim ipv6 control-message counters** command to reset IPv6 PIM control message counters.

Example # Reset IPv6 PIM control message counters on all interfaces.

```
<Sysname> reset pim ipv6 control-message counters
```

source-lifetime (IPv6 PIM view)

Syntax **source-lifetime** *interval*

undo source-lifetime

View IPv6 PIM view

Parameter *interval*: IPv6 multicast source lifetime in seconds, with an effective range of 1 to 65,535.

Description Use the **source-lifetime** command to configure the IPv6 multicast source lifetime.

Use the **undo source-lifetime** command to restore the default setting.

By default, the lifetime of an IPv6 multicast source is 210 seconds.

Related command: **state-refresh-interval (IPv6 PIM view)**.

Example # Set the IPv6 multicast source lifetime to 200 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] source-lifetime 200
```

source-policy (IPv6 PIM view)

Syntax **source-policy** *acl6-number*

undo source-policy

View IPv6 PIM view

Parameter *acl6-number*: Basic or advanced IPv6 ACL number, in the range of 2000 to 3999.

Description Use the **source-policy** command to configure an IPv6 multicast data filter.

Use the **undo source-policy** command to remove the configured IPv6 multicast data filter.

By default, no IPv6 multicast data filter is configured.

Note that:

- If you specify a basic ACL, the device filters all the received IPv6 multicast packets based on the source address, and discards packets that fail the source address match.

- If you specify an advanced ACL, the device filters all received IPv6 multicast packets based on the source and group addresses, and discards packets that fail the match.
- If this command is executed repeatedly, the last configuration will take effect.

Example # Configure the router to accept IPv6 multicast packets originated from 3121::1 and discard IPv6 multicast packets originated from 3121::2.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 3121::1 128
[Sysname-acl6-basic-2000] rule deny source 3121::2 128
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] source-policy 2000
[Sysname-pim6] quit
```

spt-switch-threshold (IPv6 PIM view)

Syntax **spt-switch-threshold** { *traffic-rate* | **infinity** } [**group-policy** *acl6-number* [**order** *order-value*]]

undo spt-switch-threshold [**group-policy** *acl6-number*]

View IPv6 PIM view

Parameter *traffic-rate*: Traffic rate threshold that will trigger RPT-to-SPT switchover, in units of kbps. The effective range is 1 to 4,194,304. This argument is not supported on a switch.

infinity: Disables RPT-to-SPT switchover.

group-policy *acl6-number*: Uses this threshold for IPv6 multicast groups that match the specified IPv6 multicast policy. In this option, *acl6-number* refers to a basic IPv6 ACL number, in the range of 2000 to 2999. If you do not include this option in your command, the threshold will apply on all IPv6 multicast groups.

order *order-value*: Specifies the order of the IPv6 ACL in the group-policy list, where *order-value* has an effective range of 1 to (the largest order value in the existing group-policy list + 1), but the value range should not include the original order value of the IPv6 ACL in the group-policy list. If you have assigned an *order-value* to a certain IPv6 ACL, do not specify the same *order-value* for another IPv6 ACL; otherwise the system will give error information. If you do not specify an *order-value*, the order value of the IPv6 ACL will remain the same in the group-policy list.

Description Use the **spt-switch-threshold** command to configure the RPT-to-SPT switchover parameters.

Use the **undo spt-switch-threshold** command to restore the default configuration.

By default, the device switches to the SPT immediately after it receives the first IPv6 multicast packet from the RPT.

Note that:

- To adjust the order of an IPv6 ACL that already exists in the group-policy list, you can use the acl6-number argument to specify this IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. The order of the other existing IPv6 ACLs in the group-policy list will remain unchanged.
- To use an IPv6 ACL that does not exist in the group-policy list, you can use the acl6-number argument to specify an IPv6 ACL and set its order-value. This will insert the IPv6 ACL to the position of order-value in the group-policy list. If you do not include the order order-value option in your command, the ACL will be appended to the end of the group-policy list.
- If you use this command multiple times on the same IPv6 multicast group, the first traffic rate configuration matched in sequence will take effect.
- For a switch, once an IPv6 multicast forwarding entry is created, subsequent IPv6 multicast data will not be encapsulated in register messages before being forwarded even if a register outgoing interface is available. Therefore, to avoid forwarding failure, do not include the **infinity** keyword in the **spt-switch-threshold** command on a switch that may become an RP (namely, a static RP or a C-RP).

Example # Set the traffic rate threshold to trigger RPT-to-SPT switchover to 4 kbps.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold 4
```

Create a group-policy with the IPv6 ACL number of 2010 and the traffic rate threshold of 100 kbps, and insert the IPv6 ACL to the first position.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] spt-switch-threshold 100 group-policy 2010 order 1
```

ssm-policy (IPv6 PIM view)

Syntax **ssm-policy** *acl6-number*

undo ssm-policy

View IPv6 PIM view

Parameter *acl6-number*: Basic IPv6 ACL number, in the range of 2000 to 2999.

Description Use the **ssm-policy** command to configure the IPv6 SSM group range.

Use the **undo ssm-policy** command to restore the system default.

By default, the IPv6 SSM group range is FF3x::/32, where x represents any legal scope.

This command allows you to define an address range of permitted or denied IPv6 multicast sources or IPv6 multicast groups. If the match succeeds, the running multicast mode will be IPv6 PIM-SSM; otherwise the multicast mode will be IPv6 PIM-SM.

Example # Configure FF3E:0:8192::/96 as the IPv6 SSM group range.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source ff3e:0:8192:: 96
[Sysname-acl6-basic-2000] quit
[Sysname] pim ipv6
[Sysname-pim6] ssm-policy 2000
```

state-refresh-hoplimit

Syntax **state-refresh-hoplimit** *hoplimit-value*

undo state-refresh-hoplimit

View IPv6 PIM view

Parameter *hoplimit-value*: Hop limit value of state refresh messages, in the range of 1 to 255.

Description Use the **state-refresh-hoplimit** command to configure the hop limit value of state refresh messages.

Use the **undo state-refresh-hoplimit** command to restore the system default.

By default, the hop limit value of state refresh messages is 255.

Related command: **pim ipv6 state-refresh-capable**, **state-refresh-interval (IPv6 PIM view)**, and **state-refresh-rate-limit (IPv6 PIM view)**.

Example # Set the hop limit value of state refresh messages to 45.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-hoplimit 45
```

state-refresh-interval (IPv6 PIM view)

Syntax **state-refresh-interval** *interval*

undo state-refresh-interval

View IPv6 PIM view

Parameter *interval*: State refresh interval in seconds, with an effective range of 1 to 255.

Description Use the **state-refresh-interval** command to configure the interval between state refresh messages.

Use the **undo state-refresh-interval** command to restore the default setting.

By default, the state refresh interval is 60 seconds.

Related command: **pim ipv6 state-refresh-capable**, **state-refresh-rate-limit (IPv6 PIM view)**, and **state-refresh-hoplimit**.

Example # Set the state refresh interval to 70 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-interval 70
```

state-refresh-rate-limit (IPv6 PIM view)

Syntax **state-refresh-rate-limit** *interval*

undo state-refresh-rate-limit

View IPv6 PIM view

Parameter *interval*: Time to wait before receiving a new refresh message, in seconds and with an effective range of 1 to 65535.

Description Use the **state-refresh-rate-limit** command to configure the time the router must wait before receiving a new state refresh message.

Use the **undo state-refresh-rate-limit** command to restore the default setting.

By default, the device waits 30 seconds before receiving a new state refresh message.

Related command: **pim ipv6 state-refresh-capable**, **state-refresh-interval (IPv6 PIM view)**, and **state-refresh-hoplimit**.

Example # Configure the device to wait 45 seconds before receiving a new state refresh message.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] state-refresh-rate-limit 45
```

static-rp (IPv6 PIM view)

Syntax **static-rp** *ipv6-rp-address* [*acl6-number*] [**preferred**]

undo static-rp *ipv6-rp-address*

View IPv6 PIM view

Parameter *ipv6-rp-address*: IPv6 address of the static RP to be configured. This address must be a valid, globally scoped IPv6 unicast address.

acl6-number: Basic IPv6 ACL number, in the range of 2000 to 2999. If you provide this argument, the configured static RP will serve only those IPv6 multicast groups that pass the filtering; otherwise, the configured static RP will serve the all IPv6 multicast groups.

preferred: Specifies to give priority to the static RP if the static RP conflicts with the dynamic RP. If you do not include the **preferred** keyword in your command, the dynamic RP will be given priority, and the static RP takes effect on if no dynamic RP exists in the network or when the dynamic RP fails.

Description Use the **static-rp** command to configure a static RP.

Use the **undo static-rp** command to configure a static RP.

By default, no static RP is configured.

Note that:

- IPv6 PIM-SM or IPv6 PIM-DM cannot be enabled on an interface that serves as a static RP.
- When the IPv6 ACL rule applied on a static RP changes, a new RP must be elected for all IPv6 multicast groups.
- You can configure multiple static RPs by carrying out this command repeatedly. However, if you carry out this command multiple times and specify the same static RP address or reference the same IPv6 ACL rule, the last configuration will override the previous one. If multiple static RPs have been configured for the same IPv6 multicast group, the one with the highest IPv6 address will be chosen to serve the group.
- You can configure up to 50 static RPs on the same device.

Related command: **display pim ipv6 rp-info**.

Example # Configure the interface with an IPv6 address of 2001::2 as a static RP.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] static-rp 2001::2
```

timer hello (IPv6 PIM view)

Syntax **timer hello** *interval*

undo timer hello

View IPv6 PIM view

Parameter *interval*: Hello interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **timer hello** command to configure the hello interval globally.

Use the **undo timer hello** command to restore the default setting.

By default, hello messages are sent at the interval of 30 seconds.

Related command: **pim ipv6 timer hello**.

Example # Set the global hello interval to 40 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer hello 40
```

timer join-prune (IPv6 PIM view)

Syntax **timer join-prune** *interval*

undo timer join-prune

View IPv6 PIM view

Parameter *interval*: Join/prune interval in seconds, with an effective range of 1 to 2,147,483,647.

Description Use the **timer join-prune** command to configure the join/prune interval globally.

Use the **undo timer join-prune** command to restore the default setting.

By default, the join/prune interval is 60 seconds.

Related command: **pim ipv6 timer join-prune**.

Example # Set the global join/prune interval to 80 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer join-prune 80
```

timer spt-switch (IPv6 PIM view)

Syntax **timer spt-switch** *interval*

undo timer spt-switch

View IPv6 PIM view

Parameter *interval*: Interval in seconds between checks of the traffic rate threshold prior to RPT-to-SPT switchover, in the range of 15 to 65,535.

Description Use the **timer spt-switch** command to configure the interval between checks of the traffic rate threshold before RPT-to-SPT switchover.

Use the **undo timer spt-switch** command to restore the default setting.

By default, the traffic rate threshold is checked at an interval of 15 seconds before RPT-to-SPT switchover.

Before using this command, be sure to use the **spt-switch-threshold** command to configure the traffic rate threshold that should trigger RPT-to-SPT switchover. Otherwise, the interval set in this command will be meaningless.

Related command: **spt-switch-threshold (IPv6 PIM view)**.

Example # Set the interval between checks of the traffic rate threshold prior to RPT-to-SPT switchover to 30 seconds.

```
<Sysname> system-view
[Sysname] pim ipv6
[Sysname-pim6] timer spt-switch 30
```

94 MULTICAST VPN CONFIGURATION COMMANDS

display multicast-domain vpn-instance share-group

Syntax **display multicast-domain vpn-instance** *vpn-instance-name* **share-group**

View Any view

Parameters *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

Description Use the **display multicast-domain vpn-instance share-group** command to view the share-group information of the specified VPN instance in the MD.

Examples # View the share-group information of VPN instance mvpn in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn share-group
MD local share-group information for VPN-Instance: mvpn
  Share-group: 225.2.2.2
  MTunnel address: 1.1.1.1
```

Table 363 Description on the fields of the display multicast-domain vpn-instance share-group command

Field	Description
Share-group	Share-group address
MTunnel address	MTI address associated with the share-group address

display multicast-domain vpn-instance switch-group receive

Syntax **display multicast-domain vpn-instance** *vpn-instance-name* **switch-group receive** [**brief** | [**active** | **group** *group-address* | **sender** *source-address* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *]

View Any view

Parameters *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

brief: Displays the brief switch-group information received by the specified VPN instance.

active: Displays the received switch-group information about active multicast domains.

group-address: Public network multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

source-address: Public network multicast source address.

vpn-source-address: VPN multicast source address.

mask: Subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.

mask-length: Mask length of the specified multicast source/group address, in the range of 0 to 32. the system default is 32.

vpn-group-address: VPN multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

Description Use the **display multicast-domain vpn-instance switch-group receive** command to view the switch-group information received by the specified VPN instance in the MD.

Related commands: **display multicast-domain vpn-instance switch-group send**.

Examples # View the switch-group information received by VPN instance mvpn in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn switch-group receive
MD switch-group information received by VPN-Instance: mvpn
Total 2 switch-groups for 8 entries

Total 2 switch-groups for 8 entries matched

switch group:  226.1.1.0 ref count: 4, active count: 2
  sender:  172.100.1.1 active count: 1
    (192.6.1.5, 239.1.1.1)       expire time: 00:03:10  active
    (192.6.1.5, 239.1.1.158)     expire time: 00:03:10
  sender:  181.100.1.1 active count: 1
    (195.6.1.2, 239.1.2.12)      expire time: 00:03:10 active
    (195.6.1.2, 239.1.2.197)     expire time: 00:03:10
switch group:  229.1.1.0 ref count: 4, active count: 2
  sender:  185.100.1.1 active count: 1
    (198.6.1.5, 239.1.3.62)      expire time: 00:03:10 active
    (198.6.1.5, 225.1.1.109)     expire time: 00:03:10
  sender:  190.100.1.1 active count: 1
    (200.6.1.2, 225.1.4.80)      expire time: 00:03:10 active
    (200.6.1.2, 225.1.4.173)     expire time: 00:03:10
```

View the brief switch-group information received by VPN instance mvpn in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn switch-group receive brief
MD switch-group information received by VPN-Instance: mvpn
Total 2 switch-groups for 8 entries

Total 2 switch-groups for 8 entries matched

switch group:  226.1.1.0 ref count: 4, active count: 2
switch group:  229.1.1.0 ref count: 4, active count: 2
```

Table 364 Description on the fields of the display multicast-domain vpn-instance switch-group receive command

Field	Description
switch group	Switch-group received
sender	BGP peer address of the PE device that sent the switch-group information
ref count	Number of VPN multicast groups referenced by the switch-group
active count	Number of active VPN multicast groups (multicast groups with active receivers) referenced by the switch-group
expire time	Remaining time of the VPN (S, G) entry referenced by the switch-group

display multicast-domain vpn-instance switch-group send

Syntax **display multicast-domain vpn-instance** *vpn-instance-name* **switch-group send** [**group** *group-address* | **reuse** *interval* | *vpn-source-address* [**mask** { *mask-length* | *mask* }] | *vpn-group-address* [**mask** { *mask-length* | *mask* }]] *

View Any view

Parameters *vpn-instance-name*: VPN instance name, a case sensitive string of up to 31 characters.

group-address: Multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

reuse *interval*: Displays the information about switch-group reuses that took place during the specified length of time in seconds. The value range of interval is 1 to 2147483647.

vpn-source-address: VPN multicast source address.

mask: Subnet mask of the specified VPN multicast source/group address, 255.255.255.255 by default.

mask-length: Mask length of the specified multicast source/group address, in the range of 0 to 32. the system default is 32.

vpn-group-address: VPN multicast group address, in the range of 224.0.1.0 to 239.255.255.255.

Description Use the **display multicast-domain vpn-instance switch-group send** command to view the switch-group information sent by the specified VPN instance in the MD.

Related commands: **display multicast-domain vpn-instance switch-group receive**.

Examples # View the switch-group information sent by VPN instance mvpn in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn switch-group send
MD switch-group information sent by VPN-Instance: mvpn
Total 2 switch-groups for 6 entries

Total 2 switch-groups for 6 entries matched

  226.1.1.0 reference_count: 3
    (192.6.1.5, 239.1.1.1)                  switch time: 00:00:21
    (192.6.1.5, 239.1.1.158)                switch time: 00:00:21
    (192.6.1.5, 239.1.2.50)                 switch time: 00:00:05
  226.1.1.1 reference_count: 3
    (192.6.1.2, 225.1.1.1)                  switch time: 00:00:21
    (192.6.1.2, 225.1.2.50)                 switch time: 00:00:05
    (192.6.1.5, 239.1.1.159)                switch time: 00:00:21
```

View the switch-group reuse information sent by VPN instance mvpn during 30 seconds in the MD.

```
<Sysname> display multicast-domain vpn-instance mvpn switch-group send reuse 30
MD switch-group information sent by VPN-Instance: mvpn
Total 2 switch-groups for 3 entries

Total 2 switch-groups for 3 entries matched

  226.1.1.0 reuse_count: 1
  226.1.1.1 reuse_count: 1
  226.1.1.2 reuse_count: 1
```

Table 365 Description on the fields of the display multicast-domain vpn-instance switch-group send command

Field	Description
reference_count	Number of VPN multicast groups referenced by the switch-group sent
switch time	Switching time of the VPN (S, G) entry referenced by the switch-group
reuse_count	Number of switch-group reuses during the specified length of time

multicast-domain holddown-time

Syntax **multicast-domain holddown-time** *interval*

undo multicast-domain holddown-time

View VPN instance view

Parameters *interval*: Backward MDT switching delay in seconds, namely the delay time for multicast traffic to be switched from the switch-MDT back to the share-MDT, in the range of 0 to 180.

Description Use the **multicast-domain holddown-time** command to configure the backward MDT switching delay.

Use the **undo multicast-domain holddown-time** command to restore the system default.

By default, the backward MDT switching delay is 60 seconds.

Note that this command cannot be configured without the previous share-MDT configuration in the VPN instance.

Examples # Set the backward MDT switching delay to 80 seconds in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain holddown-time 80
```

multicast-domain log switch-group-reuse

Syntax **multicast-domain log switch-group-reuse**

undo multicast-domain log

View VPN instance view

Parameters None

Description Use the **multicast-domain log switch-group-reuse** command to enable the switch-group reuse log function.

Use the **undo multicast-domain log switch-group-reuse** command to disable the switch-group reuse log function.

By default, the switch-group reuse log function is disabled.

Note that this command cannot be configured without the previous share-MDT configuration in the VPN instance.

Examples # Enable the switch-group reuse log function in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain log switch-group-reuse
```

multicast-domain share-group

Syntax **multicast-domain share-group** *group-address* **binding mtunnel** *mtunnel-number*

undo multicast-domain share-group

View VPN instance view

Parameters *group-address*: Multicast group address, in the range of 224.0.0.0 to 239.255.255.255.

mtunnel-number: Number of the MTI interface to be created, in the range of 0 to 127.

Description Use the **multicast-domain share-group** command to configure a share-group address and associate an MTI with the current VPN instance.

Use the **undo multicast-domain share-group** command to restore the system default.

By default, no share-group address is configured and no MTI is associated with a VPN instance.

Note that:

- On the same PE device, different VPN instances must not have the same group addresses, and *group-address* must not coincide with the switch-group address of any VPN instance; in addition, *mtunnel-number* must not coincide with the number of any MTI already created.
- This command must not be used repeatedly in the same VPN instance view. To configure a new group address and MTI for a VPN instance, you must remove the existing configuration.
- The **undo multicast-domain share-group** command removes the configured MTI and the configurations the **multicast-domain switch-group-pool**, **multicast-domain log switch-group-reuse** and **multicast-domain switch-delay** commands.
- IP multicast routing must be enabled in the VPN instance before this command can take effect.

Related commands: **multicast-domain switch-group-pool**, **multicast-domain log switch-group-reuse**, **multicast-domain switch-delay**, **multicast routing-enable** on page 1341.

Examples # Specify 224.1.1.1 as the share-group address in VPN instance mvpn and associate MTI 0 with the VPN instance.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain share-group 224.1.1.1 b
inding mtunnel 0
```

multicast-domain switch-delay

Syntax **multicast-domain switch-delay** *switch-delay*

undo multicast-domain switch-delay

View VPN instance view

Parameters *switch-delay*: MDT switching delay in seconds, namely the delay time for multicast traffic to be switched from the share-MDT to the switch-MDT, in the range of 3 to 60.

Description Use the **multicast-domain switch-delay** command to configure the MDT switching delay.

Use the **undo multicast-domain switch-delay** command to restore the system default.

By default, the MDT switching delay time is 5 seconds.

Examples # Set the MDT switching delay to 20 seconds in VPN instance mvpn.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain switch-delay 20
```

multicast-domain switch-group-pool

Syntax **multicast-domain switch-group-pool** *switch-group-pool* { *mask* | *mask-length* } [**threshold** *threshold-value* | **acl** *acl-number*] *

undo multicast-domain switch-group-pool

View VPN instance view

Parameters *switch-group-pool*: The start address of the switch-group-pool, in the range of 224.0.1.0 to 239.255.255.255.

mask: Mask for addresses in the switch-group-pool, in the range of 255.255.255.0 to 255.255.255.255, meaning the switch-group-pool contains 1 to 256 group addresses.

mask-length: Mask length for addresses in the switch-group-pool, in the range of 24 to 32, meaning the switch-group-pool contains 1 to 256 group addresses.

threshold-value: Traffic rate threshold that will trigger MDT switching, in units of kbps. The effective range is 0 to 4194304.

acl-number: Advanced ACL number, in the range of 3000 to 3999. An advanced ACL is used to define the (S, G) entry or entries to which the configured MDT switching condition will apply. If you do not specify an ACL, the configured MDT switching condition will apply to all (S, G) entries.

Description Use the **multicast-domain switch-group-pool** command to configure the address range of the switch-group-pool and the switching condition.

Use the **undo multicast-domain switch-group-pool** command to restore the system default.

By default, no switch-group-pool is configured and multicast traffic is never switched to a switch-MDT.

Note that:

- This command cannot be configured without the previous share-MDT configuration in the VPN instance.
- On a given PE device, the switch-group address range for a VPN must not contain the share-group of any VPN.
- On a given PE device, the switch-group address range for a VPN instance must not overlap with that for any other VPN instance. A new configuration with this command in the same VPN instance supersedes the existing configuration.
- The **threshold** *threshold-value* command option is not supported on a switch. If you use the **multicast-domain switch-group-pool** command on a switch, share-MDT to switch-MDT switching will take place immediately after the switch receives multicast traffic for this VPN instance.

Examples # Configure the address range of the switch-group-pool in VPN instance mvpn as 225.2.2.0 to 225.2.2.15.

```
<Sysname> system-view
[Sysname] ip vpn-instance mvpn
[Sysname-vpn-instance-mvpn] multicast-domain switch-group-pool 225.2.2.0 28
```

95 MPLS BASICS CONFIGURATION COMMANDS

- *Currently, these interface types support MPLS capability and LDP capability: serial interface, async interface, Layer 3 Ethernet interface (Ethernet interface, GE interface, and XGE interface), ATM interface, POS interface, Layer 3 virtual Ethernet interface (that is, virtual-Ethernet interface), virtual template, Mp-group interface, MFR interface, tunnel interface, VLAN interface, and virtual dial template (that is, dialer).*
- *Except for the LDP GR feature, all commands in MPLS LDP view are available in MPLS LDP VPN instance view. The difference is that the commands serves the public network LDP in MPLS LDP view but serves the MPLS LDP VPN instance in MPLS LDP VPN instance view.*
- *For information about GR commands, refer to "Basic Configuration Commands" on page 2405 and "Information Center Configuration Commands" on page 2425.*

display mpls fast-forwarding cache

Syntax **display mpls fast-forwarding cache** [**verbose**]

View Any view

Parameter **verbose**: Displays detailed information.

Description Use the **display mpls fast-forwarding cache** command to display information about the MPLS fast forwarding cache.

Example # Display information about the MPLS fast forwarding cache.

```
<Sysname> display mpls fast-forwarding cache
Fast-Forwarding Cache:  total  2  items
Label    Input_If           Output_If          Len  Flg           Used
1044     GE0/0              E2/0               4    IP            83
1049     E2/0               GE0/0              8    MPLS          81
```

Display detailed information about the MPLS fast forwarding cache.

```
<Sysname> display mpls fast-forwarding cache verbose
Fast-Forwarding Cache:  total  2  items
Label    Input_If           Output_If          Len  Flg           Used
1044     GE0/0              E2/0               4    IP            15
Fast-Forwarding Cache PreIpHead:
    FF 03 00 21
1049     E2/0               GE0/0              8    MPLS          13
Fast-Forwarding Cache PreMplsHead:
    FF 03 02 81 00 46 40 FE
```

Table 366 Description on the fields of display mpls fast-forwarding cache

Field	Description
Label	Label used as the index of the fast forwarding cache entry
Input_If	Incoming interface
Output_If	Outgoing interface
Len	Length of the pre-header, in bytes
Flg	Flag for indicating the packet type. It can be IP, MPLS, or L2VPN.
Used	Number of times the entry has been used
Fast-Forwarding Cache PreIpHead	Content of the pre-header for an IP packet
Fast-Forwarding Cache PreMPLSHead	Content of the pre-header for an MPLS packet

A pre-header is the content prefixed to a packet according to the matched entry in the fast forwarding cache. It varies depending on the type of the outgoing packet

- *For an outgoing IP packet, the pre-header is a link layer header.*
- *For an outgoing MPLS packet, the pre-header consists of a link layer header and the labels.*
- *An outgoing L2VPN packet is directly forwarded out of the outgoing interface in the matched fast forwarding entry. No pre-header is prefixed to the packet.*

display mpls ilm

Syntax **display mpls ilm** [*label*] [**include** *text*]

View Any view

Parameters *label*: Incoming label, in the range 16 to 4294967295.

include *text*: Specifies ILM entries including a specified string.

Description Use the **display mpls ilm** command to display information about the ILM table.

With no incoming label specified, the command displays the ILM entries of all incoming labels.

Examples # Display the ILM entry with a specified incoming label.

```
<Sysname> display mpls ilm 1024
Inlabel In-Interface        Token   VRF-Index Oper   LSP-Type      Swap-Label
------------------------------------------------------------------------------
1024    S2/0              2         0       POP   NORMAL        ----
    1 Record(s) Found
```

Display all ILM entries.

```
<Sysname> display mpls ilm
Inlabel In-Interface        Token   VRF-Index Oper   LSP-Type      Swap-Label
------------------------------------------------------------------------------
```

```
1024    S2/0              2         0       POP     NORMAL        ----
                  1 Record(s) Found
```

Table 367 Description on the fields of the display mpls ilm command

Field	Description
Inlabel	Incoming label
In-Interface	Incoming interface
Token	NHLFE entry index
VRF-Index	VRF index
Oper	Operation type
LSP-Type	LSP type
Swap-Label	Label for swapping

display mpls interface

Syntax **display mpls interface** [*interface-type interface-number*] [**verbose**]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

verbose: Displays detailed information.

Description Use the **display mpls interface** command to display information about a specified or all interfaces with MPLS enabled.

Related command: **display mpls statistics interface**.

Example # Display information about all interfaces with MPLS enabled.

```
<Sysname> display mpls interface
Interface   Status     TE Attr    LSP Count   CRLSP Count
Eth1/0        Up         En         0           0
Eth1/1        Up         En         0           0
```

Display detailed information about MPLS-enabled interface Ethernet 1/0.

```
<Sysname> display mpls interface ethernet 1/0 verbose
No             : 1
Interface      : Eth1/0
Status         : Down
TE Attribute   : Disable
LSPCount       : 0
CR-LSPCount    : 0
FRR            : Disabled
```

Table 368 Description on the fields of the display mpls interface command

Field	Description
No	Sequence number
Interface	Name of the interface

Table 368 Description on the fields of the display mpls interface command

Field	Description
Status	Status of the interface
TE Attr/TE Attribute	Whether TE is enabled on the interface
LSPCount	Number of LSPs on the interface
CR-LSPCount	Number of CR-LSPs on the interface
FRR	Whether FRR is enabled on the interface. If FRR is enabled, the output will also include the bound tunnels.

For information about FRR, refer to "MPLS TE Configuration Commands" on page 1565.

display mpls label

Syntax **display mpls label** { *label-value1* [**to** *label-value2*] | **all** }

View Any view

Parameter **all**: Specifies all labels.

label-value1: Specifies a label or, when used with the *label-value2* argument, the start label of a range of labels. The value of this argument ranges from 16 to 8191.

to *label-value2*: End label of a range of labels, in the range 16 to 8191.

all: Specifies all labels.

Description Use the **display mpls label** command to display the status of one or more specified or all labels.

Example # Display the status of a specified label.

```
<Sysname> display mpls label 1280
Label alloc state: '.' means not used, '$' means used
-------------Dynamic Label--------------------------------
  1280:.
```

Display the status of all labels.

```
<Sysname> display mpls label all
-----------------------------------------------------------------------
Label alloc state: '.' means not used, '$' means used
-----------------------Static Label---------------------------------
16:.... ........ ........ ........  ........ ........ ........ ........
976:........ ........ ........ ........  ........ ........
-----------------------Dynamic Label--------------------------------
1024: $ $$..... ........ ........  ........ ........ ........ ........
1088:.. ........ ........ ........  ........ ........ ........ ........
```

Table 369 Description on the fields of the display mpls label command

Field	Description
Label alloc state	Label allocation status
'.' means not used	'.' means that the label is not used
'$' means used	'$' means that the label is used
Static Label	Static labels
Dynamic Label	Dynamic labels

display mpls ldp

Syntax **display mpls ldp** [**all** [**verbose**]] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter **all**: Displays all LDP information.

verbose: Displays detailed information.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp** command to display information about LDP.

If you do not specify any parameter, the command will display all LDP information in detail.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Display all LDP information in detail.

```
<Sysname> display mpls ldp all verbose
                          LDP Global Information
------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 60 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 60 Sec
 MTU Signaling           : On           Recovery Timer       : 60 Sec

                         LDP Instance Information
 ------------------------------------------------------------------
 Instance ID            : 0          VPN-Instance         :
 Instance Status        : Active     LSR ID               : 1.1.1.1
 Hop Count Limit        : 32         Path Vector Limit    : 32
 Loop Detection         : Off
```

```
DU Re-advertise Timer  : 30 Sec     DU Re-advertise Flag : On
DU Explicit Request    : Off        Request Retry Flag   : On
Label Distribution Mode: Ordered    Label Retention Mode : Liberal
------------------------------------------------------------------
```

Table 370 Description on the fields of the display mpls ldp command

Field	Description
LDP Global Information	Global LDP information
Protocol Version	Version of the LDP protocol
Neighbor Liveliness	GR neighbor Keepalive timer
Graceful Restart	Whether GR is enabled
FT Reconnect Timer	FT reconnection timer of GR
Recovery Timer	Restore timer of GR
MTU Signaling	Whether MTU signaling is supported
LDP Instance Information	Information about LDP instances
Instance ID	Sequence number of the LDP instance
VPN-Instance	Name of the LDP-enabled VPN instance. For the default instance, nothing is displayed.
Instance Status	Status of the LDP instance
LSR ID	ID of the LSR
Hop Count Limit	Maximum hop count
Loop Detection	Whether loop detection is enabled
Path Vector Limit	Path vector maximum hop count
DU Re-advertise Flag	Whether label readvertisement is enabled for DU mode
DU Re-advertise Timer	Label readvertisement timer for DU mode
Request Retry Flag	Whether request retransmission is enabled
DU Explicit Request	Whether explicit request transmission is enabled for DU mode
Label Retention Mode	Label retention mode configured for the instance
Label Distribution Mode	Label distribution mode configured for the instance

display mpls ldp cr-lsp

Syntax **display mpls ldp cr-lsp** [**lspid** *lsr-id lsp-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter *lsr-id*: MPLS LSR ID of the device, in the format of IP address.

lsp-id: Local LSP ID of the ingress, in the range 0 to 65,535.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp cr-lsp** command to display information about CR-LSPs established by LDP.

Related command: **display mpls lsp**.

Example # Display information about CR-LSPs established by LDP.

```
<Sysname> display mpls ldp cr-lsp
        Displaying All LDP CR-LSP(s) for public network
-------------------------------------------------------------------
 CR-LSP ID      DestAddress/Mask   In/OutLabel  In/Out-Interface
-------------------------------------------------------------------
 1.1.1.9:0       2.2.2.9/32         NULL/1027    -------/S2/0
 2.2.2.9:0       1.1.1.9/32         1027/NULL    S2/0/-------
-------------------------------------------------------------------
The Total LDP CR-LSP(s): 2
```

Table 371 Description on the fields of the display mpls ldp cr-lsp command

Field	Description
CR-LSP ID	ID of the CR-LSP
DestAddress/Mask	Destination address and the mask of the FEC
In/OutLabel	Incoming label/outgoing label
In/Out-Interface	Incoming interface/outgoing interface

display mpls ldp interface

Syntax **display mpls ldp interface** [**all**] [[**vpn-instance** *vpn-instance-name*] [*interface-type interface-number*]] [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

display mpls ldp interface [**all**] [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter **all**: Displays all information.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp interface** command to display information about specified or all LDP interfaces.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Display information about all LDP interfaces.

```
<Sysname> display mpls ldp interface
     LDP Interface Information in Public Network
 ------------------------------------------------------------------------
 IF-Name         Status       LAM   Transport-Address   Hello-Sent/Rcv
 ------------------------------------------------------------------------
 Ethernet1/0     Active       DU    172.17.1.1          583/1017
 Ethernet1/1     Active       DU    172.17.1.1          578/1015
 Serial2/0       Active       DU    172.17.1.1          531/444
 ------------------------------------------------------------------------
 LAM: Label Advertisement Mode         IF-Name: Interface name
```

Display detailed information about all interfaces.

```
<Sysname> display mpls ldp interface verbose
     LDP Interface Information in Public Network
 ------------------------------------------------------------
 Interface Name : Ethernet1/0
 LDP ID         : 172.17.1.1:0          Transport Address : 172.17.1.1
 Entity Status  : Active                Interface MTU     : 1500

 Configured Hello Timer     : 15 Sec
 Negotiated Hello Timer     : 15 Sec
 Configured Keepalive Timer : 45 Sec
 Label Advertisement Mode   : Downstream Unsolicited
 Hello Message Sent/Rcvd    : 591/1033 (Message Count)
 ------------------------------------------------------------
 Interface Name : Ethernet1/1
 LDP ID         : 172.17.1.1:0          Transport Address : 172.17.1.1
 Entity Status  : Active                Interface MTU     : 1500
 Configured Hello Timer     : 15 Sec
 Negotiated Hello Timer     : 15 Sec
 Configured Keepalive Timer : 45 Sec
 Label Advertisement Mode   : Downstream Unsolicited
 Hello Message Sent/Rcvd    : 586/1031 (Message Count)
 ------------------------------------------------------------
 Interface Name : Serial2/0
 LDP ID         : 172.17.1.1:0          Transport Address : 172.17.1.1
 Entity Status  : Active                Interface MTU     : 1500
 Configured Hello Timer     : 15 Sec
 Negotiated Hello Timer     : 15 Sec
 Configured Keepalive Timer : 45 Sec
 Label Advertisement Mode   : Downstream Unsolicited
 Hello Message Sent/Rcvd    : 539/452 (Message Count)
 ------------------------------------------------------------
```

Table 372 Description on the fields of the display mpls ldp interface command

Field	Description
Interface Name	Name of an LDP-enabled interface
LDP ID	LDP identifier
Transport Address	Transport address of the entity, also used for TCP connection
Entity Status	Status of the entity, active or inactive
Interface MTU	MTU of the interface
Label Advertisement Mode	Label advertisement mode, DoD or DU
Configured Keepalive Timer	Value of the configured Keepalive timer
Configured Hello Timer	Value of the configured Hello timer
Negotiated Hello Timer	Value of the negotiated Hello timer
Hello Message Sent/Rcvd [X/Y]	X: Number of Hello messages sent from the interface
	Y: Number of Hello messages received by the interface

display mpls ldp lsp

Syntax **display mpls ldp lsp** [**vpn-instance** *vpn-instance-name* [*destination-address mask-length*]] [| { **begin** | **exclude** | **include** } *regular-expression*]

display mpls ldp lsp all [| { **begin** | **exclude** | **include** } *regular-expression*]

display mpls ldp lsp [*dest-addr mask-length*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter **all**: Displays information about all LSPs established by LDP.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

dest-addr: Destination address of the LSP.

mask-length: Length of the mask for the destination address, in the range 0 to 32.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp lsp** command to display information about LSPs established by LDP.

Related command: **display mpls ldp**.

Example # Display information about all LSPs established by LDP.

```
<Sysname> display mpls ldp lsp
                              LDP LSP Information
--------------------------------------------------------------------------------
 SN     DestAddress/Mask   In/OutLabel   Next-Hop        In/Out-Interface
--------------------------------------------------------------------------------- 1
      1.1.1.1/32         3/NULL        127.0.0.1        Ser2/0/InL0
2      10.1.1.0/24        3/NULL        10.1.1.1         Ser2/0/Eth1/1
*3      100.1.1.1/32       Liberal (1025)
--------------------------------------------------------------------------------- A
 '*' before an LSP means the LSP is not established
A '*' before a Label means the USCB or DSCB is stale
```

Table 373 Description on the fields of the display mpls ldp lsp command

Field	Description
SN	Sequence number of the LSP. A "*" before an SN means that the LSP is not established.
DestAddress/Mask	Destination address and the mask of the LSP
In/OutLabel	Incoming label/outgoing label. A "*" before an LSP means that the LSP is in the GR process. Liberal (X) means that the LSP is not available and the label value is X.
Next-Hop	Address of the next hop
In/Out-Interface	Incoming interface/outgoing interface

display mpls ldp peer

Syntax **display mpls ldp peer** [*peer-id*] [**vpn-instance** *vpn-instance-name* [**verbose**] [*peer-id*]] [| { **begin** | **exclude** | **include** } *regular-expression*]

display mpls ldp peer [**all**] [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

peer-id: LSR ID of the peer.

verbose: Displays detailed information.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

all: Display information about all peers.

Description Use the **display mpls ldp peer** command to display information about specified or all peers of the current LSR.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Display information about all peers.

```
<Sysname> display mpls ldp peer
         LDP Peer Information in Public network
Total number of peers: 3
 ------------------------------------------------------------
 Peer-ID                Transport-Address  Discovery-Source
 ------------------------------------------------------------
 172.17.1.2:0           172.17.1.2         Ethernet1/0
 168.1.1.1:0            168.1.1.1          Ethernet1/0
 100.10.1.1:0           100.10.1.1         Serial2/0
 ------------------------------------------------------------
```

Table 374 Description on the fields of the display mpls ldp peer command

Field	Description
Total number of peers	Number of peers
Peer-ID	ID of the peer
Transport-Address	Transport address of the peer
Discovery-Source	Discovery source of the peer

Display detailed information about all peers.

```
<Sysname> display mpls ldp peer verbose
        LDP Peer Information in Public network
 ------------------------------------------------------------
 Peer LDP ID         : 172.17.1.2:0
 Peer Max PDU Length : 4096            Peer Transport Address : 172.17.1.2
 Peer Loop Detection : Off             Peer Path Vector Limit : 0
 Peer FT Flag        : Off             Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----            Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Ethernet1/0
------------------------------------------------------------
 Peer LDP ID         : 168.1.1.1:0
 Peer Max PDU Length : 4096            Peer Transport Address : 168.1.1.1
 Peer Loop Detection : Off             Peer Path Vector Limit : 0
 Peer FT Flag        : Off             Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----            Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Ethernet1/1
------------------------------------------------------------
 Peer LDP ID         : 100.10.1.1:0
 Peer Max PDU Length : 4096            Peer Transport Address : 100.10.1.1
 Peer Loop Detection : Off             Peer Path Vector Limit : 0
 Peer FT Flag        : Off             Peer Keepalive Timer   : 45 Sec
 Recovery Timer      : ----            Reconnect Timer        : ----

 Peer Label Advertisement Mode : Downstream Unsolicited
 Peer Discovery Source         : Serial2/0
 ------------------------------------------------------------
```

Table 375 Description on the fields of the display mpls ldp peer verbose command

Field	Description
Peer LDP ID	LDP identifier of the peer
Peer Max PDU Length	Maximum PDU length of the peer
Peer Keepalive Timer	Keepalive timer of the peer
Peer Loop Detection	Whether loop detection is enabled on the peer
Peer Path Vector Limit	Limit of the path vector hop count configured on the peer
Peer FT Flag	Whether GR FT is enabled on the peer
Reconnect Timer	GR reconnection timer
Recovery Timer	GR recovery timer
Peer Transport Address	Transport address of the peer
Peer Label Advertisement Mode	Label advertisement mode of the peer
Peer Discovery Source	Discovery source of the peer

display mpls ldp remote-peer

Syntax **display mpls ldp remote-peer** [**remote-name** *remote-peer-name*] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter *remote-peer-name*: Name of the remote peer, a case-insensitive string of 1 to 32 characters.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp remote-peer** command to display information about LDP remote peers.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**, **remote-ip**.

Example # Display information about remote peer BJI.

```
LDP Remote Entity Information
------------------------------------------------------------------------------
 Remote Peer Name  : BJI
 Remote Peer IP    : 3.3.3.3          LDP ID : 1.1.1.1:0
 Transport Address : 1.1.1.1
 Configured Keepalive Timer : 45 Sec
 Configured Hello Timer     : 45 Sec
```

```
 Negotiated Hello Timer     : 45 Sec
 Hello Message Sent/Rcvd    : 3/2 (Message Count)
------------------------------------------------------------------------------
```

Table 376 Description on the fields of the display mpls ldp remote-peer command

Field	Description
LDP Remote Entity Information	Information about the remote LDP peer
Remote Peer Name	Name of the remote peer
Remote Peer IP	IP address of the remote peer
LDP ID	Local LDP identifier
Transport Address	Transport address of the remote peer
Configured Keepalive Timer	Targeted Keepalive timer of the peer
Configured Hello Timer	Targeted Hello timer of the peer
Negotiated Hello Timer	Negotiated Hello timer
Hello Message Sent/Rcvd	Sent: Number of Hello messages sent by the remote peer
	Rcvd: Number of Hello messages received by the remote peer

display mpls ldp session

Syntax **display mpls ldp session** [**vpn-instance** *vpn-instance-name* [**verbose**]] [*peer-id*] [| { **begin** | **exclude** | **include** } *regular-expression*]

display mpls ldp session [**all**] [**verbose**] [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter **all**: Displays all information.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters. Specify this argument to display information about all sessions of a specified VPN.

peer-id: LSR ID of the peer.

verbose: Displays detailed information.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp session** command to display information about specified or all sessions.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Display information about sessions.

```
<Sysname>display mpls ldp session
               LDP Session(s) in Public Network
Total number of sessions: 1
------------------------------------------------------------------------------
 Peer-ID            Status        LAM  SsnRole  FT   MD5  KA-Sent/Rcv
------------------------------------------------------------------------------
 1.1.1.1:0          Operational   DU   Active   Off  Off  4582/4582
------------------------------------------------------------------------------
 LAM : Label Advertisement Mode         FT  : Fault Tolerance
```

Table 377 Description on the fields of the display mpls ldp session command

Field	Description
Total number of sessions	Number of sessions
Peer-ID	LDP identifier of the peer
Status	Status of the session
LAM	Label advertisement mode of the session
SsnRole	Role of the current LSR in the session, Active or Passive
FT	Whether GR FT is enabled on the peer for the session
MD5	Whether MD5 is enabled on the peer
KA-Sent/Rcv	Number of sent Keepalives and that of received Keepalives during the session

Display detailed information about all sessions.

```
<Sysname> display mpls ldp session verbose
             LDP Session(s) in Public Network
------------------------------------------------------------------------------
 Peer LDP ID     : 1.1.1.1:0            Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 -> 1.1.1.1
 Session State   : Operational          Session Role   : Active
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---

 Negotiated Keepalive Timer        : 45 Sec
 Keepalive Message Sent/Rcvd       : 6/6 (Message Count)
 Label Advertisement Mode          : Downstream Unsolicited
 Label Resource Status(Peer/Local) : Available/Available
 Peer Discovery Mechanism          : Extended
 Session existed time              : 000:00:01  (DDD:HH:MM)
 LDP Extended Discovery Source     : Remote peer: 1

 Addresses received from peer: (Count: 2)
 10.1.1.1           1.1.1.1

------------------------------------------------------------------------------
 Peer LDP ID     : 2.2.2.2:0            Local LDP ID   : 3.3.3.3:0
 TCP Connection  : 3.3.3.3 -> 2.2.2.2
 Session State   : Operational          Session Role   : Active
 Session FT Flag : Off                  MD5 Flag       : Off
 Reconnect Timer : ---                  Recovery Timer : ---

 Negotiated Keepalive Timer        : 45 Sec
 Keepalive Message Sent/Rcvd       : 25/25 (Message Count)
```

```
Label Advertisement Mode          : Downstream Unsolicited
Label Resource Status(Peer/Local) : Available/Available
Peer Discovery Mechanism          : Basic
Session existed time              : 000:00:06  (DDD:HH:MM)
LDP Basic Discovery Source        : Ethernet1/0

Addresses received from peer: (Count: 3)
10.1.1.2            20.1.1.1            2.2.2.2

------------------------------------------------------------------------------
```

Table 378 Description on the fields of display mpls ldp session verbose

Field	Description
Peer LDP ID	LDP identifier of the peer
Local LDP ID	Local LDP identifier
TCP connection	TCP connection of the session
Session State	Status of the session
Session Role	Role of the current LSR in the session, Active or Passive
Keepalive Message Sent/Rcvd [X/Y]	X: Number of Keepalive messages sent by the current LSR during the session
	Y: Number of Keepalive messages received by the current LSR during the session
Negotiated Keep Alive Timer	Negotiated Keepalive timer
Label Advertisement Mode	Label advertisement mode of the session
Label Resource Status(Peer/Local)	Status of the label resource of the peer and that of the local label resource
Session FT Flag	Whether GR FT is enabled on the peer for the session
MD5 Flag	Whether MD5 authentication is enabled on the peer
Peer Discovery Mechanism	Discovery mechanism of the peer: Basic or Extended
Session existed time	Length of time that elapsed since the session is established
LDP Basic Discovery Source LDP Extended Discovery Source	Interface where the session is established. The value is the name of the interface for basic discovery and name of the remote peer for extended discovery.
Reconnect Timer	GR reconnection timer
Recovery Timer	GR recovery timer
Addresses received from peer	Addresses received from the peer during the session

display mpls ldp vpn-instance

Syntax **display mpls ldp vpn-instance** *vpn-instance-name* [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

|: Filters the output information.

begin: Begins with the specified string.

include: Includes the specified string.

exclude: Excludes the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters. No blank space is acceptable.

Description Use the **display mpls ldp vpn-instance** command to display information about a specified VPN instance.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Display information about VPN instance vpn1.

```
<Sysname> display mpls ldp vpn-instance vpn1
                          LDP Global Information
------------------------------------------------------------------------
 Protocol Version        : V1           Neighbor Liveness    : 60 Sec
 Graceful Restart        : Off          FT Reconnect Timer   : 60 Sec
 MTU Signaling           : On           Recovery Timer       : 60 Sec

                         LDP Instance Information
------------------------------------------------------------------------
 Instance ID             : 1            VPN-Instance         : vpn1
 Instance Status         : Active       LSR ID               : 1.1.1.9
 Hop Count Limit         : 32           Path Vector Limit    : 32
 Loop Detection          : Off
 DU Re-advertise Timer   : 30 Sec       DU Re-advertise Flag : On
 DU Explicit Request     : Off          Request Retry Flag   : On
 Label Distribution Mode : Ordered      Label Retention Mode : Liberal
```

For description on the fields of the command output, see Table 370.

display mpls lsp

Syntax **display mpls lsp** [{ **incoming-interface** | **outgoing-interface** } *interface-type interface-number*] [**in-label** *in-label-value*] [**out-label** *out-label-value*] [{ **exclude** | **include** } *dest-addr mask-length*] [**vpn-instance** *vpn-instance-name*] [**asbr** | **protocol** { **bgp** | **bgp-ipv6** | **crldp** | **ldp** | **rsvp-te** | **static** | **static-cr** }] [**egress** | **ingress** | **transit**] [**verbose**]

View Any view

Parameter **incoming-interface**: Incoming interface of the LSPs.

outgoing-interface: Outgoing interface of the LSPs.

interface-type interface-number: Specifies an interface by its type and number.

in-label-value: Value of the incoming label, in the range 0 to 1048575.

out-label-value: Value of the outgoing label, in the range 0 to 1048575.

exclude: Excludes the specified FEC.

include: Includes the specified FEC.

dest-addr: Destination address.

mask-length: Length of the mask for the destination address, in the range 0 to 32.

vpn-instance-name: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

asbr: Displays information about ASBR established LSPs.

protocol: Displays information about LSPs established by a specified protocol.

bgp: Displays information about BGP LSPs.

bgp-ipv6: Displays information about IPv6 BGP LSPs, that is, BGP4+ LSPs.

crldp: Displays information about LDP CR-LSPs.

ldp: Displays information about LDP LSPs.

rsvp-te: Displays information about CR-LSPs established by RSVP-TE.

static: Displays information about static LSPs.

static-cr: Displays information about static CR-LSPs.

egress: Displays information about LSPs taking the current LSR as egress.

ingress: Displays information about LSPs taking the current LSR as ingress.

transit: Displays information about LSPs taking the current LSR as transit LSR.

verbose: Displays detailed information.

Description Use the **display mpls lsp** command to display information about LSPs.

With no parameters specified, the command displays information about all LSPs.

Related command: **display mpls lsp**, **display mpls statistics lsp**, **display mpls static-lsp**.

This command supports these interface types: serial interface, async interface, Layer 3 Ethernet interface (Ethernet interface, GE interface, and XGE interface), ATM interface, POS interface, Layer 3 virtual Ethernet interface (that is, virtual-Ethernet interface), virtual template, Mp-group interface, MFR interface, tunnel interface, and VLAN interface.

Example # Display information about all LSPs.

```
<Sysname> display mpls lsp
------------------------------------------------------------------------------
                LSP Information: L3VPN LSP
------------------------------------------------------------------------------
FEC             In/Out Label  In/Out IF Route-Distinguisher   Vrf Name
100.1.1.1/32    1025/1024     -/-       100:1                 ASBRLSP

------------------------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------------------------
FEC             In/Out Label  In/Out IF                       Vrf Name
100.10.1.0/24   3/NULL        Eth1/0/-
100.10.1.0/24   3/NULL        Eth1/1-
168.1.0.0/16    3/NULL        S2/0/-
172.17.0.0/16   3/NULL        S2/0/-
```

Table 379 Description on the fields of the display mpls lsp command

Field	Description
FEC	Forwarding equivalence class
In/Out Label	Incoming/outgoing label
In/Out IF	Incoming/outgoing interface
Route-Distinguisher	RD
Vrf Name	Name of the VPN instance

Display detailed information about all LSPs.

```
<Sysname> display mpls lsp verbose
------------------------------------------------------------
                LSP Information: LDP LSP
------------------------------------------------------------
  No                  :  1
  VrfIndex            :
  Fec                 :  1.1.1.9/32
  Nexthop             :  127.0.0.1
  In-Label            :  3
  Out-Label           :  NULL
  In-Interface        :  Serial2/0
  Out-Interface       :  ----------
  LspIndex            :  10241
  Token               :  0
  LsrType             :  Egress
  Outgoing token      :  0
  Label Operation     :  POP
```

Table 380 Description on the fields of the display mpls lsp verbose command

Field	Description
No	Sequence number
VrfIndex	VPN instance index number
Fec	Forwarding equivalence class
Nexthop	Address of the next hop
In-Label	Incoming label
Out-Label	Outgoing label
In-Interface	Incoming interface
Out-Interface	Outgoing interface

Table 380 Description on the fields of the display mpls lsp verbose command

Field	Description
LspIndex	LSP index number
Token	Token (the pubic network)
LsrType	Role of the LSR for the LSP
Outgoing Token	Token (inter-AS VPN)

display mpls lsp statistics

Syntax **display mpls lsp statistics**

View Any view

Parameter None

Description Use the **display mpls lsp statistics** command to display LSP statistics.

Example # Display LSP statistics.

```
<Sysname> display mpls lsp statistics
Lsp Type       Total     Ingress   Transit   Egress
STATIC LSP     1         1         0         0
STATIC CRLSP   1         1         0         0
LDP LSP        0         0         0         0
CRLDP CRLSP    0         0         0         0
RSVP CRLSP     1         1         0         0
BGP LSP        0         0         0         0
ASBR LSP       0         0         0         0
BGP IPV6 LSP   0         0         0         0
------------------------------------------------------------
LSP            1         1         0         0
CRLSP          2         2         0         0
```

Table 381 Description on the fields of the display mpls lsp statistics command

Field	Description
Lsp Type	LSP Type. Available LSP types are static LSP, static CR-LSP, LDP LSP, CR-LDP CR-LSP, RSVP CR-LSP, BGP LSP, ASBR LSP, and BGP IPv6 LSP.
LSP	Grand total of LSPs
CRLSP	Grand total of CR-LSPs
Total	Total number of LSPs taking the current LSR as ingress, egress, or transit LSR
Ingress	Number of LSPs taking the current LSR as ingress
Transit	Number of LSPs taking the current LSR as transit LSR
Egress	Number of LSPs taking the current LSR as egress

display mpls nhlfe

Syntax **display mpls nhlfe** [*token*] [**include** *text*]

View Any view

Parameters *token*: NHLFE entry index. The value range varies by device.

include *text*: Specifies NHLFE entries including a specified string.

Description Use the **display mpls nhlfe** command to display information about the NHLFE table.

With the *token* argument not specified, the command displays information about all NHLFE entries.

Examples # Display information about a specified NHLFE entry.

```
<Sysname> display mpls nhlfe 2
Out-Interface       Token      Oper     Nexthop         Deep Stack
------------------------------------------------------------------------------
S2/0                  2        PUSH     88.1.1.2        1    1024
    1 Record(s) Found
```

Display all NHLFE entries.

```
<Sysname> display mpls nhlfe
Out-Interface       Token      Oper     Nexthop         Deep Stack
------------------------------------------------------------------------------
S2/0                  2        PUSH     88.1.1.2        1    1024
   1 Record(s) Found
```

Table 382 Description on the fields of the display mpls nhlfe command

Field	Description
Out-Interface	Outgoing interface
Token	NHLFE entry index
Oper	Operation type
Nexthop	Next hop
Deep	Depth of the MPLS label stack
Stack	MPLS label

display mpls route-state

Syntax **display mpls route-state** [**vpn-instance** *vpn-instance-name*] [*dest-addr mask-length*]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

dest-addr: Destination IP address.

mask-length: Length of the mask for the destination IP address, in the range 0 to 32.

Description Use the **display mpls route-state** command to display route related information.

With no VPN instance specified, the command displays route related information of the public network.

With the *dest-addr dest-mask* arguments not specified, the command displays all route related information.

Example # Display all route related information.

```
<Sysname> display mpls route-state
DEST/MASK   NEXT-HOP    OUT-INTERFACE  STATE LSP-COUNT  VPN-INDEX
------------------------------------------------------------------
1.1.1.1/32  10.0.0.1    Ser2/0           ESTA  1           0
```

Table 383 Description on the fields of the display mpls route-state command

Field	Description
DEST/MASK	Destination address and mask of the route
NEXT-HOP	Next hop on the route
OUT-INTERFACE	Outgoing interface of the route
STATE	Status of the route
LSP-COUNT	Number of LSPs
VPN-INDEX	Index number of the VPN instance

display mpls static-lsp

Syntax **display mpls static-lsp** [**lsp-name** *lsp-name*] [{ **exclude** | **include** } *dest-addr mask-length*] [**verbose**]

View Any view

Parameter *lsp-name*: Name for the LSP, a string of 1 to 15 characters.

exclude: Excludes the specified FEC.

include: Includes the specified FEC.

dest-addr: Destination IP address of the FEC.

mask-length: Length of the mask for the destination IP address, in the range 0 to 32.

verbose: Displays detailed information.

Description Use the **display mpls static-lsp** command to display information about static LSPs.

Related command: **display mpls lsp**, **display mpls statistics lsp**.

Example # Display brief information about static LSPs.

```
<Sysname> display mpls static-lsp
Name       FEC               I/O Label  I/O If                 State
lsp1       3.3.3.9/32        NULL/100   -/Eth1/0               Up
```

Table 384 Description on the fields of the display mpls static-lsp command

Field	Description
Name	Name of the LSP
FEC	Forwarding equivalence class
I/O Label	Incoming/outgoing label
I/O If	Incoming/outgoing interface
Stat	Status of the LSP

Display detailed information about static LSPs.

```
<Sysname> display mpls static-lsp verbose
No             : 1
LSP-Name       : lsp1
LSR-Type       : Ingress
FEC            : 3.3.3.9/32
In-Label       : NULL
Out-Label      : 100
In-Interface   : -
Out-Interface  : Ethernet1/0
NextHop        : 30.1.1.2
Static-Lsp Type: IPTN
Lsp Status     : Up
```

Table 385 Description on the fields of the display mpls static-lsp verbose command

Field	Description
No	Sequence number
LSP-Name	Name of the LSP
LSR-Type	Role of the LSR for the LSP, which can be ingress, egress, or transit
FEC	Forwarding equivalence class
In-Label	Incoming label
Out-Label	Outgoing label
In-Interface	Incoming interface
Out-Interface	Outgoing interface
NextHop	Address of the next hop
Static-Lsp Type	Type of the static LSP
Lsp Status	Status of the LSP

display mpls statistics interface

Syntax **display mpls statistics interface** { *interface-type interface-number* | **all** }

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

all: Displays MPLS statistics for all interfaces.

Description Use the **display mpls statistics interface** command to display MPLS statistics for a specified or all interfaces.

To display statistics, set the statistics interval first. By default, the interval is 0 and the system does not collect MPLS statistics, in which case the value of every statistical item is 0.

Related command: **statistics interval**.

Example # Display MPLS statistics for all interfaces.

```
<Sysname> display mpls statistics interface all
  Statistics for Interface IN :
  Incoming Interface Ethernet1/0
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
       Failed Label Lookup     : 0
       Start Time              : 2004/04/28  10:23:55
       End Time                : 2004/04/28  10:23:55
  Statistics for Interface OUT :
  Outgoing Interface Ethernet1/0
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
       Start Time              : 2004/04/28  10:23:55
       End Time                : 2004/04/28  10:23:55
  Statistics for Interface IN :
  Incoming Interface Ethernet1/1
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
       Failed Label Lookup     : 0
       Start Time              : 2004/04/28  10:24:04
       End Time                : 2004/04/28  10:24:04
  Statistics for Interface OUT :
  Outgoing Interface Ethernet1/1
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
       Start Time              : 2004/04/28  10:24:04
       End Time                : 2004/04/28  10:24:04
  Statistics for Interface IN :
  Incoming Interface Serial2/0
       Octets                  : 0
       Packets                 : 0
       Errors                  : 0
       Disables                : 0
```

```
     Failed Label Lookup     : 0
     Start Time              : 2004/04/28  10:24:10
     End Time                : 2004/04/28  10:24:10
Statistics for Interface OUT :
Outgoing Interface Serial2/0
     Octets                  : 0
     Packets                 : 0
     Errors                  : 0
     Disables                : 0
     Start Time              : 2004/04/28  10:24:10
     End Time                : 2004/04/28  10:24:10
```

Table 386 Description on the fields of display mpls statistics interface

Field	Description
Statistics for Interface IN	Statistics for an interface in the incoming direction
Incoming Interface Serial2/0	Incoming interface
Octets	Number of bytes received by the interface
Packets	Number of packets received by the interface
Errors	Number of inbound packet processing errors on the interface
Disables	Number of MPLS disables in the incoming direction of the interface
Failed	Number of packet label lookup failures in the incoming direction of the interface
Start Time	Start time for statistics on packets received by the interface
End Time	End time for statistics on packets received by the interface
Statistics for Interface OUT	Statistics for an interface in the outgoing direction
Octets	Number of bytes sent by the interface
Packets	Number of packets sent by the interface
Errors	Number of outbound packet processing errors on the interface
Disables	Number of MPLS disables in the outgoing direction of the interface
Start Time	Start time for statistics on packets sent by the interface
End Time	End time for statistics on packets sent by the interface

display mpls statistics lsp

Syntax **display mpls statistics lsp** { *index* | **all** | **name** *lsp-name* }

View Any view

Parameter *index*: Index number of the LSP, in the range 0 to 4294967295.

all: Specifies all LSPs.

lsp-name: Name of the LSP, a string of 1 to 15 characters.

Description Use the **display mpls statistics lsp** command to display MPLS statistics for a specified or all LSPs.

To display the statistics, set the statistics interval first. By default, the interval is 0 and the system does not collect LSP statistics, in which case the value of every statistical item is 0.

Related command: **statistics interval**.

Example # Display MPLS statistics for all LSPs.

```
<Sysname> display mpls statistics lsp all
Statistics for Lsp IN : LSP Name /LSP Index :  DynamicLsp/9217
   InSegment
       Octets                : 0
       Packets               : 0
       Errors                : 0
       Down                  : 0
       Start Time            : 2006/05/20  15:52:30
       End Time              : 2006/05/20  15:52:30
  Statistics for Lsp OUT : LSP Name /LSP Index :  DynamicLsp/9217
   OutSegment
       Octets                : 0
       Packets               : 0
       Errors                : 0
       Down                  : 0
       Start Time            : 0000/00/00  00:00:00
       End Time              : 0000/00/00  00:00:00
  Statistics for Lsp IN : LSP Name /LSP Index :  DynamicLsp/9218
   InSegment
       Octets                : 0
       Packets               : 0
       Errors                : 0
       Down                  : 0
       Start Time            : 0000/00/00  00:00:00
       End Time              : 0000/00/00  00:00:00
  Statistics for Lsp OUT : LSP Name /LSP Index :  DynamicLsp/9218
   OutSegment
       Octets                : 0
       Packets               : 0
       Errors                : 0
       Down                  : 0
       Start Time            : 2006/05/20  15:52:30
       End Time              : 2006/05/20  15:52:30
```

Table 387 Description on the fields of the display mpls statistics lsp command

Field	Description
Statistics for Lsp IN : LSP Name /LSP Index : DynamicLsp/10241	Statistics for LSP DynamicLsp/10241 in the incoming direction
InSegment	Information about the LSP in the incoming direction
OutSegment	Information about the LSP in the outgoing direction
Octets	Bytes of data processed
Packets	Number of packets processed
Errors	Number of errors
Down	Number of packets discarded
Start Time	Start time of the statistics
End Time	End time of the statistics

- *For an ingress, no statistics is collected in the incoming direction and the start time and end time in the InSegment part of the command output are both 0.*
- *Similarly, for an egress, no statistics is collected in the outgoing direction and the start time and end time in the OutSegment part of the command output are both 0.*

du-readvertise

Syntax **du-readvertise**

undo du-readvertise

View MPLS LDP view/MPLS LDP VPN instance view

Parameter None

Description Use the **du-readvertise** command to enable label readvertisement for DU mode.

Use the **undo du-readvertise** command to restore the default.

By default, label readvertisement is enabled in DU mode.

Example # Enable DU mode label readvertisement for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] du-readvertise
```

Enable DU mode label readvertisement for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] du-readvertise
```

du-readvertise timer

Syntax **du-readvertise timer** *value*

undo du-readvertise timer

View MPLS LDP view/MPLS LDP VPN instance view

Parameter *value*: Label readvertisement interval in seconds. It ranges from 1 to 65,535.

Description Use the **du-readvertise timer** command to set the interval for label readvertisement in DU mode.

Use the **undo du-readvertise timer** command to restore the default.

By default, the interval for label readvertisement in DU mode is 30 seconds.

Example # Set the DU mode label readvertisement interval to 100 seconds for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] du-readvertise timer 100
```

Set the DU mode label readvertisement interval to 100 seconds for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] du-readvertise timer 100
```

graceful-restart (MPLS LDP view)

Syntax **graceful-restart**

undo graceful-restart

View MPLS LDP view

Parameter None

Description Use the **graceful-restart** command to enable MPLS LDP Graceful Restart (GR).

Use the **undo graceful-restart** command to disable MPLS LDP GR.

By default, MPLS LDP GR is disabled.

Note that enabling and disabling GR may remove all the sessions and instances and the LSPs based on the sessions, which need to be reestablished.

Example # Enable MPLS LDP GR.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart
```

graceful-restart mpls ldp

Syntax **graceful-restart mpls ldp**

View User view

Parameter None

Description Use the **graceful-restart mpls ldp** command to gracefully restart MPLS LDP.

Note that:

- This command is used to test MPLS LDP GR without main/backup failover. It is not recommended in normal cases.
- The MPLS LDP GR capability is required for this command to take effect.

Related commands: **graceful-restart (MPLS LDP view)**.

Example # Gracefully restart MPLS LDP.

```
<Sysname> graceful-restart mpls ldp
```

graceful-restart timer neighbor-liveness

Syntax **graceful-restart timer neighbor-liveness** *timer*

undo graceful-restart timer neighbor-liveness

View MPLS LDP view

Parameter *timer*: LDP neighbor liveness time, in the range 60 to 300 seconds.

Description Use the **graceful-restart timer neighbor-liveness** command to set the LDP neighbor liveness time.

Use the **undo graceful-restart timer neighbor-liveness** command to restore the default.

By default, the LDP neighbor liveness time is 120 seconds.

Note that:

- Modifying the LDP neighbor liveness time removes the existing sessions and the LSPs based on the sessions, which need to be reestablished.
- For LDP sessions with MD5 authentication configured, you need to increase the LDP neighbor liveness time appropriately so that the TCP connection can be reestablished.

Example # Set the LDP neighbor liveness time to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer neighbor-liveness 100
```

graceful-restart timer reconnect

Syntax **graceful-restart timer reconnect** *timer*

undo graceful-restart timer reconnect

View MPLS LDP view

Parameter *timer*: Fault Tolerance (FT) reconnect time, in the range 60 to 300 seconds.

Description Use the **graceful-restart timer reconnect** command to set the FT reconnect time.

Use the **undo graceful-restart timer reconnect** command to restore the default.

By default, the FT reconnect time is 300 seconds.

Note that:

- The FT reconnect time refers to the maximum time that the stale state flag will be preserved by the LSR after the TCP connection fails.
- Modifying the FT reconnect time may cause all original sessions to be reestablished. LSPs based on the sessions will be removed and need to be reestablished.

Example # Set the FT reconnect time to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer reconnect 100
```

graceful-restart timer recovery

Syntax **graceful-restart timer recovery** *timer*

undo graceful-restart timer recovery

View MPLS LDP view

Parameter *timer*: LDP recovery time, in the range 3 to 300 seconds.

Description Use the **graceful-restart timer recovery** command to set the LDP recovery time.

Use the **undo graceful-restart timer recovery** command to restore the default.

By default, the LDP recovery time is 300 seconds.

Note that:

- The LDP recovery time refers to the maximum time that the stale state label will be kept by the LSR after a TCP reconnection.

- Modifying the LDP recovery time may cause the original sessions to be reestablished. The LSPs based on the sessions will be removed and need to be reestablished.

Example # Set the LDP recovery time to 45 seconds.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] graceful-restart timer recovery 45
```

hops-count

Syntax **hops-count** *hop-number*

undo hops-count

View MPLS LDP view/MPLS LDP VPN instance view

Parameter *hop-number*: Hop count, in the range 1 to 32.

Description Use the **hops-count** command to set the maximum hop count for loop detection.

Use the **undo hops-count** command to restore the default.

By default, the maximum hop count for loop detection is 32.

Note that:

- You must configure the command before enabling LDP on any interface.
- The maximum hop count dictates how fast LDP detects a loop. Adjust this argument as required.

Related command: **loop-detect**, **path-vectors**.

Example # Set the maximum hop count for loop detection to 25 for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] hops-count 25
```

Set the maximum hop count for loop detection to 25 for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] hops-count 25
```

label advertise

Syntax **label advertise** { **explicit-null** | **implicit-null** | **non-null** }

undo label advertise

View MPLS view

Parameter **explicit-null**: Specifies that the egress does not support PHP and distributes to the penultimate hop an explicit null label, whose value is 0.

implicit-null: Specifies that the egress supports PHP and distributes to the penultimate hop an implicit null label, whose value is 3.

non-null: Specifies that the egress distributes the label to the penultimate hop normally and does not support PHP. The value of the distributed label will be equal to or greater than 1024.

Description Use the **label advertise** command to specify whether the egress supports PHP and what type of label the egress should distribute to the penultimate hop.

Use the **undo label advertise** command to restore the default.

By default, an egress supports PHP and distributes to the penultimate hop an implicit null label.

- *The type of label for the egress to distribute depends on whether the penultimate hop supports PHP.*
- *You must use the **reset mpls ldp** command to reset LDP sessions for the configuration to take effect.*

Example # Specify the egress to distribute an explicit null label to the penultimate hop.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] label advertise explicit-null
```

label-distribution

Syntax **label-distribution** { **independent** | **ordered** }

undo label-distribution

View MPLS LDP view/MPLS LDP VPN instance view

Parameter **independent**: Works in independent mode, advertising label bindings anytime.

ordered: Works in ordered mode, advertising to its upstream a label binding only when it receives a specific label binding message from the next hop for a FEC or the LSR itself is the egress node of the FEC.

Description Use the **label-distribution** command to configure the label distribution control mode.

Use the **undo label-distribution** command to restore the default.

The default mode is **ordered**.

*You must use the **reset mpls ldp** command to reset LDP sessions for the configuration to take effect.*

Example # Set the label distribution control mode to independent for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] label-distribution independent
```

Set the label distribution control mode to independent for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] label-distribution independent
```

label-retention

Syntax **label-retention** { **conservative** | **liberal** }

undo label-retention

View MPLS LDP view/MPLS LDP VPN instance view

Parameter **conservative**: Works in conservative mode, keeping only label to FEC bindings that are from its next hops for the FECs

liberal: Works in liberal mode, keeping any received label to FEC binding regardless of whether the binding is from its next hop for the FEC or not.

Description Use the **label-retention** command to configure the label retention mode.

Use the **undo label-retention** command to restore the default.

The default label retention mode is **liberal**.

*You must use the **reset mpls ldp** command to reset LDP sessions for the configuration to take effect.*

Example # Set the label retention mode to conservative for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] label-retention conservative
```

Set the label retention mode to conservative for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] label-retention conservative
```

loop-detect

Syntax **loop-detect**

undo loop-detect

View MPLS LDP view/MPLS LDP VPN instance view

Parameter None

Description Use the **loop-detect** command to enable loop detection.

Use the **undo loop-detect** command to disable loop detection.

By default, loop detection is disabled.

Note that you must enable loop detection before enabling LDP on any interfaces.

Related command: **hops-count**, **path-vectors**.

Example # Enable loop detection for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] loop-detect
```

Enable loop detection for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] loop-detect
```

lsp-trigger

Syntax **lsp-trigger** { **all** | **ip-prefix** *prefix-name* }

undo lsp-trigger { **all** | **ip-prefix** *prefix-name* }

View MPLS view

Parameter **all**: Specifies all FECs, that is, all static routes and IGP routes.

prefix-name: Name of the IP address prefix list, a string of 1 to 19 characters.

Description Use the **lsp-trigger** command to configure the LSP establishment triggering policy.

Use the **undo lsp-trigger** command to restore the default.

By default, only loopback addresses with 32-bit masks can trigger LDP to establish LSPs.

Note that:

- With the **all** keyword specified in the **lsp-trigger** command, all static and IGP routes can trigger LDP to establish LSPs.
- Using **ip-prefix** *prefix-name* keyword and argument combination in the **lsp-trigger** command, only IGP routes surviving the IGP route filtering based on an IP address prefix list can trigger LDP to establish LSPs.
- For an LSP to be established, an exactly matched routing entry must exist on the LSR. With loopback addresses using 32-bit masks, only exactly matched host routing entries can trigger LDP to establish LSPs.
- An IP address prefix list affects only static routes and IGP routes.
- For information about IP address prefix list, refer to "IP Addressing Configuration Commands" on page 781.

Example # Specify LDP to allow all static and IGP routes to trigger LSP establishment.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] lsp-trigger all
```

lsr-id

Syntax **lsr-id** *lsr-id*

undo lsr-id

View MPLS LDP view/MPLS LDP VPN instance view

Parameter *lsr-id*: LDP LSR ID.

Description Use the **lsr-id** command to configure an LDP LSR ID.

Use the **undo lsr-id** command to remove a configured LDP LSR ID and all LDP sessions.

By default, the LDP LSR ID takes the value of the MPLS LSR ID.

Example # Configure the LDP LSR ID of the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] lsr-id 2.2.2.3
```

Configure the LDP LSR ID of LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] lsr-id 4.2.2.3
```

md5-password

Syntax **md5-password** { **cipher** | **plain** } *peer-lsr-id password*

undo md5-password *peer-lsr-id*

View MPLS LDP view/MPLS LDP VPN instance view

Parameter **cipher**: Displays the password in cipher text.

plain: Displays the password in plain text.

peer-lsr-id: MPLS LSR ID of the peer. An LSR and its peer use the same password.

password: Password string, case sensitive. If you specify the **plain** keyword, it must be a string of 1 to 16 characters in plain text. If you specify the **cipher** keyword, it can be either a string of 1 to 16 characters in plain text or a string of 24 characters in cipher text.

Description Use the **md5-password** command to enable LDP MD5 authentication and set the password, which must be the same as that configured on the peer.

Use the **undo md5-password** command to disable LDP MD5 authentication.

By default, LDP MD5 authentication is disabled.

Changing of the password will cause the session to be reestablished and all existing LSPs related to the session to be deleted.

This command takes effect only when MPLS LDP is enabled in the corresponding view.

Example # Enable MD5 authentication for the public network LDP, setting the password display mode to plain text.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] md5-password plain 3.3.3.3 beijingpass
```

Enable MD5 authentication for LDP instance named vpn1, setting the password display mode to plain text.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] md5-password plain 3.3.3.3 beijingpass
```

mpls

Syntax **mpls**

undo mpls

View System view/interface view

Parameter None

Description Use the **mpls** command in system view to enable MPLS for the current node and enter MPLS view.

Use the **undo mpls** command in system view to disable MPLS for the current node.

Use the **mpls** command in interface view to enable MPLS for the interface.

Use the **undo mpls** command in interface view to disable MPLS for the interface.

By default, MPLS capability is not enabled.

Note that:

- You need to configure the LSR ID before enabling MPLS capability.
- You need to enable MPLS globally before enabling it for an interface.
- You need to enter MPLS view to configure other MPLS commands.

Related command: **mpls lsr-id**.

Example # Enable MPLS for the current node and enter MPLS view.

```
<Sysname> System-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
```

Enable MPLS for interface Ethernet 1/0.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
```

mpls ldp (system view)

Syntax **mpls ldp** [**vpn-instance** *vpn-instance-name*]

undo mpls ldp [**vpn-instance** *vpn-instance-name*]

View System view

Parameter *vpn-instance-name*: Name of the VPN instance, a case-sensitive string of 1 to 31 characters.

Description Use the **mpls ldp** command to enable LDP for the current node and enter MPLS LDP view.

Use the **undo mpls ldp** command to disable LDP for the current node and remove all LDP instances

Use the **mpls ldp vpn-instance** command to enable LDP for a VPN instance, create an LDP instance, and enter MPLS LDP VPN instance view.

Use the **undo mpls ldp vpn-instance** command to disable LDP for a VPN instance.

Configure the **mpls ldp** command after configuring MPLS LSR ID and enabling MPLS for the current node.

Example # Enable LDP for the current node.

```
<Sysname> System-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] quit
[Sysname] mpls ldp
[Sysname-mpls-ldp]
```

Enable LDP for VPN instance vpn1.

```
<Sysname> System-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1]
```

mpls ldp (interface view)

Syntax **mpls ldp**

undo mpls ldp

View Interface view

Parameter None

Description Use the **mpls ldp** command to enable LDP on an interface.

Use the **undo mpls ldp** command to disable LDP on an interface.

By default, LDP is disabled on an interface.

After you enable LDP on an interface, the interface will create an entity and periodically sends Hello messages.

Before enabling LDP in interface view, be sure to complete the following tasks:

- Use the **mpls** command in system view to enable MPLS.
- Use the **mpls ldp** command in system view to enable MPLS LDP.
- Use the **mpls** command in interface view to enable MPLS.

If the interface is bound to a VPN instance, you must use the **mpls ldp vpn-instance** command to enable LDP for the VPN instance before enabling LDP on the interface to add the interface into the VPN instance.

This command supports these interface types: serial interface, async interface, Layer 3 Ethernet interface (Ethernet interface, GE interface, and XGE interface), ATM interface, POS interface, Layer 3 virtual Ethernet interface (that is, virtual-Ethernet interface), virtual template, Mp-group interface, MFR interface, tunnel interface, VLAN interface, and virtual dial template (that is, dialer).

Example # Enable LDP for interface Ethernet 1/0.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls ldp
```

mpls ldp advertisement

Syntax **mpls ldp advertisement** { **dod** | **du** }

undo mpls ldp advertisement

View Interface view

Parameter **dod**: Works in downstream on demand (DoD) mode, advertising a label to FEC binding in response to the explicit request of an upstream LSR.

du: Works in downstream unsolicited (DU) mode, advertising label to FEC bindings to LSRs without explicitly requesting bindings.

Description Use the **mpls ldp advertisement** command to specify the label advertisement mode.

Use the **undo mpls ldp advertisement** command to restore the default.

By default, DU mode is used.

Note that changing the label advertisement mode will cause the existing sessions to be reestablished, and the LSPs established by the sessions to be deleted and reestablished.

Example # Set the label advertisement mode to DoD.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls ldp
[Sysname-Ethernet1/0] mpls ldp advertisement dod
```

mpls ldp remote-peer

Syntax **mpls ldp remote-peer** *remote-peer-name*

undo mpls ldp remote-peer *remote-peer-name*

View System view

Parameter *remote-peer-name*: Name of the remote peer, a case-insensitive string of 1 to 32 characters.

Description Use the **mpls ldp remote-peer** command to create a remote peer entity and enter MPLS LDP remote peer view.

Use the **undo mpls ldp remote-peer** command to remove a remote peer entity.

Related command: **remote-ip**.

Example # Create a remote peer entity named BJI.

```
<Sysname> System-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji]
```

mpls ldp timer hello-hold

Syntax **mpls ldp timer hello-hold** *value*

undo mpls ldp timer hello-hold

View Interface view/MPLS LDP remote peer view

Parameter *value*: Length of time for the Hello timer, in the range 1 to 65,535 seconds.

Description Use the **mpls ldp timer hello-hold** command to set the Hello timers.

Use the **undo mpls ldp timer hello-hold** command to restore the defaults.

In interface view, you configure the link Hello timer; in MPLS LDP remote peer view, you configure the targeted Hello timer.

By default, the value of the link Hello timer is 15 seconds, while that of the targeted Hello timer is 45 seconds.

Changing the values of the Hello timers does not affect any existing session.

Related command: **mpls ldp (system view)**, **mpls ldp (interface view)**.

Example # Set the link Hello timer for local sessions to 100 seconds on interface Ethernet 1/0.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls ldp
[Sysname-Ethernet1/0] mpls ldp timer hello-hold 100
```

Set the targeted Hello timer for remote sessions to 1,000 seconds.

```
<Sysname> System-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp timer hello-hold 1000
```

mpls ldp timer keepalive-hold

Syntax **mpls ldp timer keepalive-hold** *value*

undo mpls ldp timer keepalive-hold

View Interface view/MPLS LDP remote peer view

Parameter *value*: Length of time for the Keepalive timer, in the range 1 to 65,535 seconds.

Description Use the **mpls ldp timer keepalive-hold** command to set the keepalive timers.

Use the **undo mpls ldp timer keepalive-hold** command to restore the defaults.

In interface view, you configure the link Keepalive timer; in MPLS LDP remote peer view, you configure the targeted Keepalive timer.

By default, both the link Keepalive timer and targeted Keepalive timer are set to 45 seconds.

CAUTION:

- *If more than one link with LDP enabled exists between two LSRs when, for example, the two LSRs are connected through multiple interfaces, the Keepalive timers of all the links must be identical for sessions to be stable.*
- *Changing the values of the Keepalive timers will cause existing LDP sessions to be reestablished.*

Example # Set the link Keepalive timer for local sessions to 50 seconds on interface Ethernet 1/0.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls ldp
[Sysname-Ethernet1/0] mpls ldp timer keepalive-hold 50
```

Set the targeted Keepalive timer for remote sessions to 1,000 seconds.

```
<Sysname> System-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp timer keepalive-hold 1000
```

mpls ldp transport-address

Syntax **mpls ldp transport-address** { *interface-type interface-number* | **interface** }

undo mpls ldp transport-address

View Interface view/MPLS LDP remote peer view

Parameter *interface-type interface-number*: Specifies an interface by its type and number, making LDP use the address of this interface as the TCP transport address.

interface: Specifies that LDP use the IP address of the current interface as the TCP transport address. This keyword is available only in interface view.

Description Use the **mpls ldp transport-address** command to configure the LDP transport addresses.

Use the **undo mpls ldp transport-address** command to restore the defaults.

By default, the transport addresses are both the MPLS LSR ID.

In interface view, you configure the link Hello transport address; in MPLS LDP remote peer view, you configure the targeted Hello transport address.

Example # On interface Ethernet 1/0, configure the link Hello transport address for local sessions as the IP address of the current interface.

```
<Sysname> System-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls ldp
[Sysname-Ethernet1/0] mpls ldp transport-address interface
```

Configure the targeted Hello transport address for remote sessions to be the IP address of interface Ethernet 1/0.

```
[Sysname] mpls ldp remote-peer bji
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
[Sysname-mpls-ldp-remote-bji] mpls ldp transport-address ethernet 1/0
```

mpls lsr-id

Syntax **mpls lsr-id** *lsr-id*

undo mpls lsr-id

View System view

Parameter *lsr-id*: ID for identifying the LSR, in dotted decimal notation.

Description Use the **mpls lsr-id** command to configure the ID of an LSR.

Use the **undo mpls lsr-id** command to remove the ID of an LSR.

By default, no LSR ID is configured.

Your must configure the LSR ID of an LSR before configuring any other MPLS commands.

You are recommended to use the address of a loopback interface on the LSR as the ID.

Related command: **display mpls interface**.

Example # Set the LSR ID to 3.3.3.3.

```
<Sysname> system-view
[Sysname] mpls lsr-id 3.3.3.3
```

mtu-signalling

Syntax **mtu-signalling**

undo mtu-signalling

View MPLS LDP view

Parameter None

Description Use the **mtu-signalling** command to enable MTU signaling.

Use the **undo mtu-signalling** command to disable MTU signaling.

By default, MTU signaling is enabled.

Enabling/disabling MTU signaling will cause the existing sessions to be reestablished, and the LSPs established by the sessions to be deleted and reestablished.

Example # Enable MTU signaling.

```
<Sysname> System-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] mtu-signalling
```

path-vectors

Syntax **path-vectors** *pv-number*

undo path-vectors

View MPLS LDP VPN instance view/MPLS LDP view

Parameter *pv-number*: Path vector maximum hop count, in the range 1 to 32.

Description Use the **path-vectors** command to set the path vector maximum hop count.

Use the **undo path-vectors** command to restore the default.

By default, the path vector maximum hop count for an instance is 32.

Note that this command takes effect only when MPLS LDP is enabled on all interfaces.

Related command: **loop-detect**, **hops-count**.

Example # Set the path vector maximum hop count to 3 for the public network LDP.

```
<Sysname> system-view
[Sysname] mpls ldp
[Sysname-mpls-ldp] path-vectors 3
```

Set the path vector maximum hop count to 3 for LDP instance named vpn1.

```
<Sysname> system-view
[Sysname] mpls ldp vpn-instance vpn1
[Sysname-mpls-ldp-vpn-instance-vpn1] path-vectors 3
```

ping lsp

Syntax **ping lsp** [**-a** *source-ip* | **-c** *count* | **-exp** *exp-value* | **-h** *ttl-value* | **-m** *wait-time* | **-r** *reply-mode* | **-s** *packet-size* | **-t** *time-out* | **-v**] * { **ipv4** *dest-addr mask-length* [*destination-ip-addr-header*] | **te** *interface-type interface-number* }

View Any view

Parameter **-a** *source-ip*: Specifies the source address for the echo request message.

-c *count*: Specifies the number of attempts to sending the request message. The *count* argument ranges from 1 to 4,294,967,295.

-exp *exp-value*: Specifies the EXP value for the echo request message. The *exp-value* argument ranges from 0 to 7.

-h *ttl-value*: Specifies the TTL value for the echo request message. The *ttl-value* argument ranges from 1 to 255.

-m *wait-time*: Specifies the interval for sending echo request messages. The *wait-time* argument ranges from 1 to 10,000.

-r *reply-mode*: Specifies the reply mode in response to an echo request message. The *reply-mode* argument can be 1 or 2. A value of 1 means "Do not response", while a value of 2 means "Respond using a UDP packet".

-s *packet-size*: Specifies the payload length of the echo request message. The *packet-size* argument ranges from 64 to 8,100.

-t *time-out*: Specifies the timeout interval for the response to an echo request message. The *time-out* argument ranges from 0 to 65,535.

-v: Displays detailed response information.

ipv4 *dest-addr mask-length*: Specifies the LDP Ipv4 destination address and the mask. The *mask-length* argument ranges from 0 to 32.

destination-ip-addr-header: Specifies the IP header destination address for the MPLS echo request message, which can be any address on segment 127.0.0.0/8, that is, any local loopback address.

te *interface-type interface-number*: Specifies a tunnel interface by its type and number.

Description Use the **ping lsp** command to check the validity and reachability of an LSP.

Example # Ping a specified address by send five packets.

```
<Sysname> ping lsp -c 5 ipv4 3.3.3.9 32
LSP PING FEC: LDP IPV4 PREFIX 3.3.3.9/32 : 100  data bytes, press CT
RL_C to break
    Reply from 100.1.2.1: bytes=100 Sequence=0 time = 31 ms
    Reply from 100.1.2.1: bytes=100 Sequence=1 time = 62 ms
    Reply from 100.1.2.1: bytes=100 Sequence=2 time = 62 ms
    Reply from 100.2.3.1: bytes=100 Sequence=3 time = 62 ms
    Reply from 100.1.2.1: bytes=100 Sequence=4 time = 62 ms

  --- FEC: LDP IPV4 PREFIX 3.3.3.9/32 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 31/55/62 ms
```

remote-ip

Syntax **remote-ip** *ip-address*

undo remote-ip

View MPLS LDP remote peer view

Parameter *ip-address*: IP address of the remote peer.

Description Use the **remote-ip** command to configure the LDP remote peer IP address.

Use the **undo remote-ip** command to remove the configuration.

Note that the LDP remote peer IP address must be the MPLS LSR ID of the remote peer. Two peers use their respective MPLS LSR ID as the transport addresses to establish the TCP connection.

Related command: **mpls ldp remote-peer**.

Example # Configure the LDP remote peer IP address.

```
<Sysname> system-view
[Sysname] mpls ldp remote-peer BJI
[Sysname-mpls-ldp-remote-bji] remote-ip 3.3.3.3
```

reset mpls fast-forwarding cache

Syntax **reset mpls fast-forwarding cache**

View User view

Parameter None

Description Use the **reset mpls fast-forwarding cache** command to clear information in the MPLS fast forwarding cache.

Example # Clear information in the MPLS fast forwarding cache.

```
<Sysname> reset mpls fast-forwarding cache
```

reset mpls ldp

Syntax **reset mpls ldp** [**all** | [**vpn-instance** *vpn-instance-name*] [*fec mask* | **peer** *peer-id*]]

View User view

Parameter **all**: Specifies all LDP instances, including the public ones and private ones.

vpn-instance *vpn-instance-name*: Specifies a VPN instance by its name, a case-sensitive string of 1 to 31 characters.

fec mask: Specifies a FEC by the destination IP address and mask.

peer *peer-id*: Specifies a peer by its LSR ID.

Description Use the **reset mpls ldp** command to reset LDP sessions.

With no parameters specified, the command resets the sessions of all public network LDP instances.

Example # Reset the sessions of all public network LDP instances.

```
<Sysname> reset mpls ldp
```

Reset the sessions of all LDP instances.

```
<Sysname> reset mpls ldp all
```

Reset the sessions of LDP instance vpn1.

```
<Sysname> reset mpls ldp vpn-instance vpn1
```

Reset the sessions of a specified FEC.

```
<Sysname> reset mpls ldp 2.2.2.2 24
```

Reset the sessions with a specified peer.

```
<Sysname> reset mpls ldp peer 2.2.2.9
```

reset mpls statistics interface

Syntax **reset mpls statistics interface** { *interface-type interface-number* | **all** }

View User view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

all: Specifies all interfaces.

Description Use the **reset mpls statistics interface** command to clear MPLS statistics for a specified or all MPLS interfaces.

Related command: **display mpls statistics interface**.

Example # Clear MPLS statistics for interface Ethernet 1/0.

```
<Sysname> reset mpls statistics interface ethernet 1/0
```

reset mpls statistics lsp

Syntax **reset mpls statistics lsp** { *index* | **all** | **name** *lsp-name* }

View User view

Parameter *index*: Index number of the LSP, in the range 0 to 4,294,967,295.

all: Specifies all LSPs.

lsp-name: Name of the LSP, a string of 1 to 15 characters.

Description Use the **reset mpls statistics lsp** command to clear MPLS statistics for a specified or all LSPs.

Related command: **display mpls statistics lsp**.

Example # Clear MPLS statistics for LSP lsp1.

```
<Sysname> reset mpls statistics lsp lsp1
```

snmp-agent trap enable mpls

Syntax **snmp-agent trap enable mpls**

undo snmp-agent trap enable mpls

View System view

Parameter None

Description Use the **snmp-agent trap enable mpls** command to enable the MPLS trap function.

Use the **undo snmp-agent trap enable** command to disable the function.

By default, the function is disabled.

Example # Enable the MPLS trap function.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable mpls
```

static-lsp egress

Syntax **static-lsp egress** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label*

undo static-lsp egress *lsp-name*

View System view

Parameter *lsp-name*: Name for the LSP, a string of 1 to 15 characters.

interface-type interface-number: Specifies an interface by its type and number.

in-label: Incoming label value, in the range 16 to 1,023.

Description Use the **static-lsp egress** command to configure a static LSP taking the current LSR as the egress.

Use the **undo static-lsp egress** command to remove a static LSP taking the current LSR as the egress.

Related command: **static-lsp ingress**, **static-lsp transit**, **display mpls static-lsp**.

Example # Configure a static LSP named bj-sh, taking the current LSR as the egress.

```
<Sysname> system-view
[Sysname] static-lsp egress bj-sh incoming-interface serial 2/0 in-label 233
```

static-lsp ingress

Syntax **static-lsp ingress** *lsp-name* { **destination** *dest-addr* { *mask* | *mask-length* } } { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label*

undo static-lsp ingress *lsp-name*

View System view

Parameter *lsp-name*: Name for the LSP, a string of 1 to 15 characters.

dest-addr: Destination IP address of the LSP.

mask: Mask of the destination IP address.

mask-length: Length of the mask for the destination address, in the range 0 to 32.

next-hop-addr: Address of the next hop.

interface-type interface-number: Specifies an interface by its type and number.

out-label: Outgoing label value, in the range 16 to 1023.

Description Use the **static-lsp ingress** command to configure a static LSP taking the current LSR as the ingress.

Use the **undo static-lsp ingress** command to remove a static LSP taking the current LSR as the ingress.

Note that:

- If you specify the next hop when configuring a static LSP, and the address of the next hop is present in the routing table, you must also specify the next hop when configuring the static IP route.

- If you specify the outgoing interface when configuring a static LSP, you must also specify the outgoing interface when configuring the static IP route.
- The address of the next hop cannot be any local public network IP address.

Related command: **static-lsp egress**, **static-lsp transit**, **display mpls static-lsp**.

Example # Configure a static LSP to destination address 202.25.38.1, taking the current LSR as the ingress.

```
<Sysname> system-view
[Sysname] static-lsp ingress bj-sh destination 202.25.38.1 24 nextho
p 202.55.25.33 out-label 237
```

static-lsp transit

Syntax **static-lsp transit** *lsp-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label*

undo static-lsp transit *lsp-name*

View System view

Parameter *lsp-name*: Name for the LSP, a string of 1 to 15 characters.

incoming-interface *interface-type interface-number*: Specifies an incoming interface by its type and number.

in-label: Incoming label value, in the range 16 to 1023.

next-hop-addr: Address of the next hop.

outgoing-interface *interface-type interface-number*: Specifies an outgoing interface by its type and number.

out-label: Outgoing label value, in the range 16 to 1023.

Description Use the **static-lsp transit** command to configure a static LSP taking the current LSR as a transit LSR.

Use the **undo static-lsp transit** command to remove a static LSP taking the current LSR as a transit LSR.

Note that:

- If you specify the next hop when configuring a static LSP, and the address of the next hop is present in the routing table, you must also specify the next hop when configuring the static IP route.
- If you specify the outgoing interface when configuring a static LSP, you must also specify the outgoing interface when configuring the static IP route.
- The address of the next hop cannot be any local public network IP address.

Related command: **static-lsp egress**, **static-lsp ingress**.

Example # Configure a static LSP, taking interface Serial 2/0 as the incoming interface and setting the incoming label as 123 and the outgoing label as 253.

```
<Sysname> system-view
[Sysname] static-lsp transit bj-sh incoming-interface serial 2/0 in-
label 123 nexthop 202.34.114.7 out-label 253
```

statistics interval

Syntax **statistics interval** *interval-time*

undo statistics interval

View MPLS view

Parameter *interval-time*: Statistics Interval, in the range 30 to 65,535 seconds.

Description Use the **statistics interval** command to set the statistics interval, that is, the interval for collecting statistics.

Use the **undo statistics interval** command to restore the default.

By default, the interval is 0.

Related command: **display mpls statistics interface**, **display mpls statistics lsp**.

Example # Set the statistics interval to 30 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] statistics interval 30
```

tracert lsp

Syntax **tracert lsp** [**-a** *source-ip* | **-exp** *exp-value* | **-h** *ttl-value* | **-r** *reply-mode* |**-t** *time-out*] * { **ipv4** *dest-addr mask-length* [*destination-ip-addr-header*] | **te** *interface-type interface-number* }

View Any view

Parameter **-a** *source-ip*: Specifies the source address for the echo request message.

-exp *exp-value*: Specifies the EXP value for the echo request message. The *exp-value* argument ranges from 0 to 7.

-h *ttl-value*: Specifies the TTL value for the echo request message. The *ttl-value* argument ranges from 1 to 255.

-r *reply-mode*: Specifies the reply mode in response to an echo request message. The *reply-mode* argument can be 1 or 2. A value of 1 means "Do not response", while a value of 2 means "Respond using a UDP packet".

-t *time-out*: Specifies the timeout interval for the response to an echo request message. The *time-out* argument ranges from 0 to 65,535 milliseconds.

ipv4 *dest-addr mask*: Specifies the LDP Ipv4 destination address and the mask. The *mask* argument ranges from 0 to 32.

destination-ip-addr-header: Specifies the IP header destination address for the MPLS echo request message, which can be any address on segment 127.0.0.0/8, that is, any local loopback address.

te *interface-type interface-number*: Specifies a tunnel interface by its type and number.

Description Use the **tracert lsp** command to locate an MPLS LSP error.

Example # Locate an error along the LSP to 3.3.3.9 on host 1.1.1.1.

```
<Sysname> tracert lsp ipv4 3.3.3.9 32
LSP Trace Route FEC: LDP IPV4 PREFIX 3.3.3.9/32 , press CTRL_C to break.
  TTL   Replier            Time    Type      Downstream
  0                                Ingress   10.4.5.1/[1025]
  1     10.4.5.1           1       Transit   100.3.4.1/[1024]
  2     100.1.4.2          63      Transit   100.1.2.1/[3]
  3     100.1.2.1          129     Egress
```

ttl expiration

Syntax **ttl expiration pop**

undo ttl expiration pop

View MPLS view

Parameter None

Description Use the **ttl expiration pop** command to specify that the ICMP response message be transported back along the IP route when the TTL of an MPLS packet expires.

Use the **undo ttl expiration pop** command to specify that the ICMP response be transported back along the LSP when the TTL of an MPLS packet expires.

By default, the ICMP response message of an MPLS packet with a one-level label is transported back along the IP route.

Note that configuring the **undo mpls** command will remove the configuration of the **ttl expiration pop** command.

Related command: **ttl propagate**.

Example # Specify that the ICMP response be transported back along the LSP when the TTL of an MPLS packet expires

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] undo ttl expiration pop
```

ttl propagate

Syntax **ttl propagate { public | vpn }**

undo ttl propagate { public | vpn }

View MPLS view

Parameter **public**: Enables MPLS IP TTL propagation for public network packets.

vpn: Enables MPLS IP TTL propagation for VPN packets.

Description Use the **ttl propagate** command to enable MPLS IP TTL propagation for either public network packets or VPN packets.

Use the **undo ttl propagate** command to disable the function.

By default, MPLS IP TTL propagation is enabled for only public network packets.

Related command: **ttl expiration**.

Example # Enable MPLS IP TTL propagation for VPN packets.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] ttl propagate vpn
```

96 MPLS TE CONFIGURATION COMMANDS

MPLS TE is available on these interfaces: synchronous/asynchronous serial interface (Serial), asynchronous serial interface (Async), Layer 3 Ethernet interface (Ethernet, GE, XGE), ATM interface, POS interface, Layer 3 virtual Ethernet interface (Virtual-Ethernet), virtual template interface, MP group interface, MFR interface, tunnel interface, and VLAN interface.

add hop

Syntax **add hop** *ip-address1* [**include** [**loose** | **strict**] | **exclude**] { **after** | **before** } *ip-address2*

View Explicit path view

Parameter *ip-address1*: IP address or Router ID of the node to be inserted in the explicit path, in dotted decimal notation.

include: Includes the specified IP address in the explicit path.

loose: Indicates that the next hop is a loose node which is not necessarily directly connected to the specified node.

strict: Indicates that the next hop is a strict node which must be directly connected to the specified node.

exclude: Excludes the node identified by the *ip-address1* argument from the explicit path. Excluded addresses are not considered in path calculation.

after: Inserts the node identified by the *ip-address1* argument after the reference node.

before: Inserts the node identified by the *ip-address1* argument before the reference node.

ip-address2: IP address of the reference node, in dotted decimal notation.

Description Use the **add hop** command to insert a node to the explicit path.

By default, the specified node is included in the explicit path and its next hop is a strict node.

Example # Insert 3.3.29.3 behind 3.3.10.5 on the explicit path PL and exclude this IP address in path calculation.

```
<Sysname> system-view
[Sysname] explicit-path path1
[Sysname-explicit-path-path1] add hop 3.3.29.3 exclude after 3.3.10.5
```

delete hop

Syntax **delete hop** *ip-address*

View Explicit path view

Parameter *ip-address*: IP address of a node along the explicit path.

Description Use the **delete hop** command to remove a specified node from the explicit path.

Example # Remove the node identified by 10.0.0.1 from the explicit path PL.

```
<Sysname> system-view
[Sysname] explicit-path path1
[Sysname-explicit-path-path1] delete hop 10.0.0.1
```

display explicit-path

Syntax **display explicit-path** [*pathname*]

View Any view

Parameter *pathname*: Specifies a path name, a string of 1 to 31 characters.

Description Use the **display explicit-path** command to display information about an explicit path.

If no path name is specified, information about all explicit paths is displayed.

Example # Display information about all explicit paths.

```
<Sysname> display explicit-path
Path Name : ErHop-Path1  Path Status : Enabled
 1             1.1.1.10         Strict                    Include
 2             2.1.1.10         Strict                    Include
 3             1.1.1.20         Strict                    Include
 4             2.1.1.20         Strict                    Include
 5             2.1.1.30         Strict                    Include
 6             1.1.1.30         Strict                    Include
 7             9.4.4.4          Strict                    Include
Path Name : ErHop-Path2  Path Status : Enabled
 1             1.1.1.10         Strict                    Include
 2             2.1.1.10         Strict                    Include
 3             1.1.1.40         Strict                    Include
 4             2.1.1.40         Strict                    Include
 5             1.1.1.50         Strict                    Include
 6             2.1.1.40         Strict                    Include
```

```
7               2.1.1.30          Strict                      Include
8               1.1.1.30          Strict                      Include
9               9.4.4.4           Strict                      Include
```

Table 388 Description on the fields of the display explicit-path command

Field	Description
Path Name	Explicit path name
Path Status	Explicit path status

display isis traffic-eng advertisements

Syntax **display isis traffic-eng advertisements** [**level-1** | **level-1-2** | **level-2**] [**lsp-id** *lsp-id* | **local**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameter **level-1**: Displays the TE information of IS-IS Level-1 routers.

level-1-2: Displays the TE information of IS-IS Level-1-2 routers.

level-2: Displays the TE information of IS-IS Level-2 routers.

lsp-id *lsp-id*: Specifies a link state packet ID (LSP ID) to display the TE information advertised by it. For more information about IS-IS LSP, refer to "IS-IS Configuration Commands" on page 1037.

local: Displays local TE information.

process-id: Specifies an IS-IS process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a string of 1 to 31 characters. For the default VPN instance, you do not need to configure this keyword and argument combination.

Description Use the **display isis traffic-eng advertisements** command to display the latest TE information advertised by IS-IS TE.

If no IS-IS level is specified, the TE information of IS-IS Level-1-2 routers is displayed.

Example # Display the latest TE information advertised by IS-IS TE.

```
<Sysname> display isis traffic-eng advertisements
                            TE information for ISIS(1)
                            --------------------------

Level-1 Link State Database
---------------------------

LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x00000001   0x3f57        534           0/0/0

 NLPID      : IPV4
 AREA ADDR  : 00.0005
```

```
 INTF ADDR  : 10.1.1.1
 INTF ADDR  : 1.1.1.9
 INTF ADDR  : 30.1.1.1

Level-2 Link State Database
---------------------------

LSPID                 LSP Seq Num  LSP Checksum  LSP Holdtime  ATT/P/OL
0000.0000.0001.00-00* 0x0000001c   0xf1ec        687           0/0/0

 NLPID      : IPV4
 AREA ADDR  : 00.0005
 INTF ADDR  : 10.1.1.1
 INTF ADDR  : 1.1.1.9
 INTF ADDR  : 30.1.1.1
 Router ID  : 1.1.1.9
+NBR        : 0000.0000.0002.02  COST: 10
    Admin Group: 0x00000000
    Interface IP Address:  10.1.1.1
    Physical BW  :      12500 Bytes/sec
    Reservable BW:       6250 Bytes/sec
    Unreserved BW for Class Type 0:
    BW Unresrv[0]:       6250 Bytes/sec BW Unresrv[1]:       6250 Bytes/sec
    BW Unresrv[2]:       6250 Bytes/sec BW Unresrv[3]:       6250 Bytes/sec
    BW Unresrv[4]:       6250 Bytes/sec BW Unresrv[5]:       6250 Bytes/sec
    BW Unresrv[6]:       6250 Bytes/sec BW Unresrv[7]:       6250 Bytes/sec
    Unreserved BW for Class Type 1:
    BW Unresrv[0]:          0 Bytes/sec BW Unresrv[1]:          0 Bytes/sec
    BW Unresrv[2]:          0 Bytes/sec BW Unresrv[3]:          0 Bytes/sec
    BW Unresrv[4]:          0 Bytes/sec BW Unresrv[5]:          0 Bytes/sec
    BW Unresrv[6]:          0 Bytes/sec BW Unresrv[7]:          0 Bytes/sec
    TE Cost      :         10
    Bandwidth Constraint Model: Russian Doll
    Bandwidth Constraints:
    BC[0]        :       6250 Bytes/sec BC[1]        :          0 Bytes/sec
    Local Overbooking Multiplier:
    LOM[0]       :        100 %         LOM[1]       :        100 %
+NBR        : 0000.0000.0004.00  COST: 10
    Admin Group: 0x00000000
    Interface IP Address:  30.1.1.1
    Peer IP Address     :  30.1.1.2
    Physical BW  :      12500 Bytes/sec
    Reservable BW:       6250 Bytes/sec
    Unreserved BW for Class Type 0:
    BW Unresrv[0]:       6250 Bytes/sec BW Unresrv[1]:       6250 Bytes/sec
    BW Unresrv[2]:       6250 Bytes/sec BW Unresrv[3]:       6250 Bytes/sec
    BW Unresrv[4]:       6250 Bytes/sec BW Unresrv[5]:       6250 Bytes/sec
    BW Unresrv[6]:       6250 Bytes/sec BW Unresrv[7]:       6250 Bytes/sec
    Unreserved BW for Class Type 1:
    BW Unresrv[0]:          0 Bytes/sec BW Unresrv[1]:          0 Bytes/sec
    BW Unresrv[2]:          0 Bytes/sec BW Unresrv[3]:          0 Bytes/sec
    BW Unresrv[4]:          0 Bytes/sec BW Unresrv[5]:          0 Bytes/sec
    BW Unresrv[6]:          0 Bytes/sec BW Unresrv[7]:          0 Bytes/sec
    TE Cost      :         10
    Bandwidth Constraint Model: Russian Doll
    Bandwidth Constraints:
    BC[0]        :       6250 Bytes/sec BC[1]        :          0 Bytes/sec
    Local Overbooking Multiplier:
    LOM[0]       :        100 %         LOM[1]       :        100 %
```

Table 389 Description on the fields of display isis traffic-eng advertisements

Field	Description
LSPID	LSP ID
LSP Seq Num	LSP sequence number

Table 389 Description on the fields of display isis traffic-eng advertisements

Field	Description
LSP Checksum	LSP checksum
LSP Holdtime	LSP holdtime
ATT/P/OL	Attach bit (ATT)
	Partition bit (P)
	Overload bit (OL)
NLPID	Network protocol type
AREA ADDR	IS-IS area address
INTF ADDR	Interface address
Router ID	Router ID
+NBR	Neighbor
COST	Cost
Admin Group	Link administrative group attribute
Interface IP Address	Interface IP address
Physical BW	Physical bandwidth
Reservable BW	Reservable bandwidth
BW Unresrv[0]-[7]	Available subpool bandwidths at eight levels
TE Cost	TE cost
Bandwidth Constraint Model	Bandwidth constraint model
BC[0]	Global pool
BC[1]	Subpool
Local Overbooking Multiplier	Local overbooking multiplier
LOM[0] LOM[1]	Local overbooking multiplier. The bracketed number indicates the level of bandwidth.
Peer IP Address	Peer IP address

display isis traffic-eng link

Syntax **display isis traffic-eng link** [**level-1** | **level-1-2** | **level-2**] [**verbose**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameter **level-1**: Displays the TE information of IS-IS Level-1 routers.

level-1-2: Displays the TE information of IS-IS Level-1-2 routers.

level-2: Displays the TE information of IS-IS Level-2 routers.

verbose: Displays details.

process-id: IS-IS process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a string of 1 to 31 characters. For the default VPN instance, you do not need to configure this keyword and argument combination.

Description Use the **display isis traffic-eng link** command to display information about TE links for IS-IS.

If no IS-IS level is specified, the TE link information of IS-IS Level-1-2 routers is displayed.

Example # Display information about TE links for IS-IS.

```
<Sysname> display isis traffic-eng link
                          TE information for ISIS(1)
                          --------------------------
Level-2 Link Information
------------------------
 0000.0000.0001.00-->0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0002.00-->0000.0000.0003.00    Type: P2P     LinkID: 3.3.3.9
 0000.0000.0002.00-->0000.0000.0001.01    Type: MULACC  LinkID: 10.1.1.1
 0000.0000.0003.00-->0000.0000.0002.00    Type: P2P     LinkID: 2.2.2.9
 0000.0000.0003.00-->0000.0000.0004.01    Type: MULACC  LinkID: 30.1.1.2
 0000.0000.0004.00-->0000.0000.0004.01    Type: MULACC  LinkID: 30.1.1.2
 Total Number of TE Links in Level-2 Area: 6, Num Active: 6
```

Table 390 Description on the fields of the display mpls lsp statistics command

Field	Description
Type	Link type
LinkID	Link ID
Total Number of TE Links in Level-2 Area	Total number of TE links in the Level-2 area
Num Active	Number of active TE links

display isis traffic-eng network

Syntax **display isis traffic-eng network** [**level-1** | **level-1-2** | **level-2**] [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameter **level-1**: Displays the TE information of IS-IS Level-1 routers.

level-1-2: Displays the TE information of IS-IS Level-1-2 routers.

level-2: Displays the TE information of IS-IS Level-2 routers.

process-id: IS-IS process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a string of 1 to 31 characters. For the default VPN instance, you do not need to configure this keyword and argument combination.

Description Use the **display isis traffic-eng network** command to display information about TE networks for IS-IS.

If no IS-IS level is specified, the TE network information in the IS-IS Level-1-2 area is displayed.

Example # Display information about TE networks for IS-IS.

```
<Sysname> display isis traffic-eng network
                          TE information for ISIS(1)
                          --------------------------
Level-1 Network Information
---------------------------
    DIS Router ID  : 89.1.1.1        DIS's Ip Address         : 86.1.1.1
    Status In CSPF : ACTIVE          Attached Router Count    : 2
    List of Attached Routers
 RouterId : 89.1.1.1   Nbr : 1111.1111.1111.00  Link State : 1
 RouterId : 89.2.2.2   Nbr : 1111.1111.1113.00  Link State : 1
 Total Number of TE Networks in Level-1 Area: 1, Num Active: 1
Level-2 Network Information
---------------------------
    DIS Router ID  : 89.1.1.1        DIS's Ip Address         : 86.1.1.1
    Status In CSPF : ACTIVE          Attached Router Count    : 2
    List of Attached Routers
 RouterId : 89.1.1.1   Nbr : 1111.1111.1111.00  Link State : 1
 RouterId : 89.2.2.2   Nbr : 1111.1111.1113.00  Link State : 1
 Total Number of TE Networks in Level-2 Area: 1, Num Active: 1
```

Table 391 Description on the fields of the display isis traffic-eng network command

Field	Description
Level-1 Network Information	Level-1 network information
DIS Router ID	DR router ID
DIS's Ip Address	IP address of the DR router
Status In CSPF	CSPF state
Attached Router Count	Number of attached routers
List of Attached Routers	List of attached routers
RouterId	Router ID
Nbr	Neighbors
Link State	Link state
Total Number of TE Networks in Level-1 Area	Total number of TE networks in the Level-1 area
Num Active	Number of active TE links
Level-2 Network Information	Level-2 network information
Total Number of TE Networks in Level-2 Area	Total number of TE networks in the Level-2 area

display isis traffic-eng statistics

Syntax **display isis traffic-eng statistics** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameter *process-id*: IS-IS process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a string of 1 to 31 characters. For the default VPN instance, you do not need to configure this keyword and argument combination.

Description Use the **display isis traffic-eng statistics** command to display the statistics about TE for IS-IS.

If no IS-IS level is specified, the statistics about TE in the IS-IS Level-1-2 area is displayed.

Example # Display statistics about TE for IS-IS.

```
<Sysname> display isis traffic-eng statistics
                            TE information for ISIS(1)
                            --------------------------
TE Statistics Information
-------------------------
 IS-IS System Type                          : Level-1-2
 IS-IS Cost Style Status                    : Wide
 IS-IS Level-1 Traffic Engineering Status   : Disabled
 IS-IS Level-2 Traffic Engineering Status   : Enabled
 IS-IS Router ID                            : 1.1.1.9
```

Table 392 Description on the fields of the display isis traffic-eng statistics command

Field	Description
IS-IS System Type	System type
IS-IS Cost Style Status	Cost type of the router
IS-IS Level-1 Traffic Engineering Status	TE state of Level-1 router
IS-IS Level-2 Traffic Engineering Status	TE state of Level-2 router
IS-IS Router ID	IS-IS router ID

display isis traffic-eng sub-tlvs

Syntax **display isis traffic-eng sub-tlvs** [*process-id* | **vpn-instance** *vpn-instance-name*]

View Any view

Parameter *process-id*: IS-IS process ID, in the range 1 to 65535.

vpn-instance *vpn-instance-name*: Specifies a VPN instance. The *vpn-instance-name* argument is a string of 1 to 31 characters. For the default VPN instance, you do not need to configure this keyword and argument combination.

Description Use the **display isis traffic-eng sub-tlvs** command to display information about sub-TLVs for the IS-IS TE extension.

If no IS-IS level is specified, information about TE extension sub-TLVs in the IS-IS Level-1-2 area is displayed.

Related command: **te-set-subtlv**.

Example # Display TE sub-TLV information for IS-IS.

```
<Sysname> display isis traffic-eng sub-tlvs
IS-IS(1) SubTlv Information
--------------------------------
 Unreserved sub-pool bandwidth sub-tlv value : 251
 Bandwidth constraint sub-tlv value          : 252
 LO multiplier sub-tlv value                 : 253
```

Table 393 Description on the fields of the display isis traffic-eng statistics command

Field	Description
Unreserved sub-pool bandwidth sub-tlv value	Sub-TLV of unreserved subpool bandwidth
Bandwidth constraint sub-tlv value	Bandwidth constraint sub-TLV
LO multiplier sub-tlv value	LOM sub-TLV

display mpls rsvp-te

Syntax **display mpls rsvp-te** [**interface** [*interface-type interface-number*] [**|** { **begin** | **include** | **exclude** } *regular-expression*]]

View Any view

Parameter **interface**: Displays RSVP-TE configuration for interfaces. If no interface is specified, the RSVP-TE configuration of all RSVP-TE enabled interfaces is displayed.

interface-type interface-number: Specifies an interface for which RSVP-TE configuration is displayed.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te interface** command to display RSVP-TE configuration.

If the **interface** is not specified, the global RSVP-TE configuration is displayed.

Example # Display the global RSVP-TE configuration.

```
<Sysname> display mpls rsvp-te
LSR ID: 4.4.4.4
 Resv Confirmation Request: DISABLE
 RSVP Hello Extension: ENABLE
 Hello interval: 3 sec         Max Hello misses: 3
 Path and Resv message refresh interval: 30 sec
 Path and Resv message refresh retries count: 3
```

```
 Blockade Multiplier: 4
Graceful Restart: ENABLE
 Restart Time: 200 sec       Recovery Time: 150 sec
```

Table 394 Description on the fields of the display mpls rsvp-te command

Field	Description
LSR ID	Label switched Router ID, in the format of X.X.X.X
Resv Confirmation Request	Reserved confirmation request
RSVP Hello Extension	State of the hello mechanism: enabled or disabled
Hello Interval	Hello interval, in seconds
Max Hello misses	Maximum number of consecutive hello losses before a neighbor is considered dead
Path and Resv message refresh interval	Path and reservation message refresh interval, in seconds
Path and Resv message refresh retries count	Number of Path and Resv message retransmissions
Blockade Multiplier	Blockade multiplier
Graceful Restart	State of GR: enabled or disabled
Restart Time	GR restart interval in seconds
Recovery Time	GR recovery interval in seconds

Display the RSVP-TE configuration on interface Ethernet 1/0.

```
<Sysname> display mpls rsvp-te interface ethernet 1/0
Interface Ethernet1/0
 Interface state: UP
 Total-BW: 80              Used-BW: 20
 Hello configured: NO      Num of Neighbors: 1
 SRefresh feature: ENABLE  SRefresh Interval: 30sec
 Authentication: DISABLE   Reliability configured: NO
 Retransmit Interval: 500msec  Increment Value: 1
```

Table 395 Description on the fields of the display mpls rsvp-te interface command

Field	Description
Interface Ethernet1/0	RSVP-TE enabled interface
Interface state	Physical interface state
Total-BW	Total bandwidth (in kbps)
Used-BW	Used bandwidth (in kbps)
Hello configured	State of the hello mechanism: enabled or disabled
Num of Neighbors	Number of neighbors connected to the interface
Srefresh feature	State of the summary refresh function: enabled or disabled
Srefresh interval	Summary refresh interval (in seconds)
Authentication	State of authentication: enabled or disabled
Reliability	Whether the reliability feature is configured: yes or no
Retransmit interval	Initial retransmission interval (in milliseconds)
Increment value	Increment value delta which governs the speed with which the interface increases the retransmission interval

display mpls rsvp-te established

Syntax **display mpls rsvp-te established** [**interface** *interface-type interface-number*] [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te established** command to display information about RSVP-TE globally or for an interface.

Example # Display RSVP-TE information for interface Ethernet 1/0.

```
<Sysname> display mpls rsvp-te established interface ethernet 1/0
Interface Ethernet1/0
 Token Bucket Rate: 0.00            Peak Data Rate: 0.00
 Tunnel Dest: 2.2.2.2               Ingress LSR ID: 3.3.3.3
 Local LSP ID: 4                    Session Tunnel ID: 4
 Next Hop Addr: 80.4.1.1
 Upstream Label: 1024               Downstream Label: 3
```

Table 396 Description on the fields of the display mpls rsvp-te established command

Field	Description
Interface Ethernet1/0	RSVP-TE enabled Ethernet interface
Token Bucket rate	Token bucket rate, a traffic parameter
Peak Data Rate	Peak rate, a traffic parameter
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
Local LSP ID	Local LSP ID
Session Tunnel ID	Session tunnel ID
Next Hop Addr	Next hop address, in the format of X.X.X.X
Upstream label	Upstream label
Downstream Label	Downstream label

display mpls rsvp-te peer

Syntax **display mpls rsvp-te peer** [**interface** *interface-type interface-number*] [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te peer** command to display information about RSVP-TE neighbors on the specified or all interfaces.

Example # Display information about RSVP-TE neighbors on all interfaces.

```
<Sysname> display mpls rsvp-te peer
Interface Ethernet1/0
 Neighbor Addr: 80.4.1.1
 SrcInstance: 841             NbrSrcInstance: 928
 PSB Count: 0                 RSB Count: 1
 Hello Type Sent: ACK         Neighbor Hello Extension: ENABLE
 SRefresh Enable: NO          Reliability Enable: YES
 Graceful Restart State: Ready
 Restart Time: 200 sec        Recovery Time: 150 sec

Interface Ethernet1/1
 Neighbor Addr: 80.2.1.1
 SrcInstance: 832             NbrSrcInstance: 920
 PSB Count: 1                 RSB Count: 0
 Hello Type Sent: REQ         Neighbor Hello Extension: ENABLE
 SRefresh Enable: NO          Reliability Enable: YES
 Graceful Restart State: Not ready
 Restart Time: ---            Recovery Time: ---
```

Table 397 Description on the fields of the display mpls rsvp-te peer command

Field	Description
Interface Ethernet1/0	RSVP-TE enabled Ethernet interface
Neighbor Addr:	Neighbor address, in the format of X.X.X.X.
SrcInstance	Instance of source Message ID
NbrSrcInstance	Instance of neighbor Message ID
PSB Count	Number of path state blocks

Table 397 Description on the fields of the display mpls rsvp-te peer command

Field	Description
RSB Count	Number of reservation state blocks
Hello Type Sent	Type of hellos sent to the neighbor: REQ, ACK, or NONE
Neighbor Hello Extension	State of hello extension: enabled or disabled. This field is displayed only when hello extension is enabled on the interface.
SRefresh Enable	State of summary refresh: YES for enabled and NO for disabled
Reliability Enable	State of the reliability function: YES for enabled and NO for disabled
Graceful Restart State	Neighbor's GR status: Not ready, Ready, Restart, or Recovery. Displayed as --- when not supported by the device.
Restart Time	GR restart interval in seconds
Recovery Time	GR recovery interval in seconds

display mpls rsvp-te psb-content

Syntax **display mpls rsvp-te psb-content** *ingress-lsr-id lspid tunnel-id egress-lsr-id* [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter *ingress-lsr-id*: Ingress LSR ID.

lspid: Local LSR ID, in the range 1 to 65,535.

tunnel-id: Tunnel ID, in the range 0 to 65,535.

egress-lsr-id: Egress LSR ID.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te psb-content** command to display information about RSVP-TE PSB.

Example # Display PSB information.

```
<Sysname> display mpls rsvp-te psb-content 19.19.19.19 1 0 29.29.29.29
The PSB Content:
 Tunnel Dest: 29.29.29.29     Session Tunnel ID: 0
 Tunnel ExtID: 19.19.19.19
 Ingress LSR ID: 19.19.19.19  Local LSP ID: 1
 Previous Hop : 101.101.101.1 Next Hop : -----
 Incoming / Outgoing Interface: Ethernet1/0  /  -----
```

```
 InLabel : 3            OutLabel : NULL
Send Message ID : 1      Recv Message ID : 0
 Session Attribute-
   SetupPrio: 7         HoldPrio: 7
   SessionFlag: SE Style desired
  ERO Information-
     L-Type          ERO-IPAddr       ERO-PrefixLen
   ERHOP_STRICT    101.101.101.2         32
 RRO Information-
   RRO-CType: IPV4   RRO-IPAddress: 101.101.101.1   RRO-IPPrefixLen: 32
 SenderTspec Information-
   Token bucket rate: 0.00
   Token bucket size: 0.00
   Peak data rate: 0.00
   Minimum policed unit: 0
   Maximum packet size: 4294967295
 Path Message arrive on Ethernet1/0 from PHOP 101.101.101.1
 Resource Reservation OK
 Graceful Restart State: Stale
```

Table 398 Description on the fields of display mpls rsvp-te psb content

Field	Description
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Session Tunnel ID	Session tunnel ID
Tunnel ExtID	Tunnel extension ID, in the format of X.X.X.X
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
Local LSP ID	Local LSP ID
Next Hop	Next hop address, in the format of X.X.X.X
Previous Hop	Previous hop address, in the format of X.X.X.X
In Label	Incoming label
Out Label	Outgoing label
Send message ID	Instance of sent Message ID
Resv Message ID	Instance of received Message ID
Setup Prio	Session setup priority
HoldPrio	Session hold priority
Session Flag	Session flag (local protection policy, label, SE style)
ERO Information	Information about explicit routes
L-Type	Explicit routing type: strict or loose
ERO-IPAddress	IP address for an explicit route
ERO-Prefix Len	Prefix length for an explicit route
RRO Information	Information about route recording
RRO-C Type	Type of route recording
RRO-IP Address	IP address of recorded route in the format of X.X.X.X
RRO-IPPrefixLen	IP prefix length of recorded route
Sender Tspec Information	Information about sender's service specifications
Token Bucket rate	Token bucket rate (in kbps), a traffic parameter
Token Bucket size	Token bucket size, a traffic parameter
Peak Data Rate	Peak data rate (in kbps), a traffic parameter
Maximum packet size	Maximum packet size, a traffic parameter
Minimum policed unit	Minimum policed unit, a traffic parameter

Table 398 Description on the fields of display mpls rsvp-te psb content

Field	Description
Path message	Path message sent from the interface to the next hop at X.X.X.X
Resource	Available when the RSVP flag is configured
Graceful Restart State	State of GR: stale or normal. Displayed as --- when not supported by the device.

display mpls rsvp-te request

Syntax **display mpls rsvp-te request** [**interface** *interface-type interface-number*] [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te request** command to display information about RSVP-TE requests on the specified or all interfaces.

Example # Display information about RSVP-TE requests on all interfaces.

```
<Sysname> display mpls rsvp-te request
Interface Ethernet1/0:
 Tunnel Dest: 2.2.2.2                Ingress LSR ID: 3.3.3.3
 Local LSP ID: 4                     Session Tunnel ID: 4
 NextHopAddr: 80.4.1.1
 SessionFlag: SE Style desired.
 Token bucket rate: 0.00             Token bucket size: 1000.00
 Out Interface: Ethernet1/1
```

Table 399 Description on the fields of the display mpls rsvp-te request command

Field	Description
Interface Ethernet1/0	RSVP-TE enabled Ethernet interface
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
Local LSP ID	Local LSP ID
Session Tunnel ID	Session tunnel ID

Table 399 Description on the fields of the display mpls rsvp-te request command

Field	Description
Next Hop Address	Next hop address, in the format of X.X.X.X
SessionFlag	Reservation style
Token Bucket rate	Token bucket rate, a traffic parameter
Token Bucket Size	Token bucket size, a traffic parameter
Out Interface	Output interface

display mpls rsvp-te reservation

Syntax **display mpls rsvp-te reservation** [**interface** *interface-type interface-number*] [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te reservation** command to display information about RSVP-TE reservations on the specified or all interfaces.

Example # Display information about RSVP-TE reservations on interface Ethernet 1/0.

```
<Sysname> display mpls rsvp-te reservation interface ethernet 1/0
Interface Ethernet1/0
 Tunnel Dest: 29.29.29.29     Ingress LSR ID: 19.19.19.19
 LSP ID: 1                    Tunnel ID: 1
 Upstream Label: -----
 Token bucket rate: 0.00       Token bucket size: 0.00
```

Display information about RSVP-TE reservations on all interfaces.

```
<Sysname> display mpls rsvp-te reservation
Interface Ethernet1/0
 Tunnel Dest: 29.29.29.29     Ingress LSR ID: 19.19.19.19
 LSP ID: 1                    Tunnel ID: 1
 Upstream Label: -----
 Token bucket rate: 0.00       Token bucket size: 0.00
 Interface: Outgoing-Interface at the Egress
 Tunnel Dest: 19.19.19.19     Ingress LSR ID: 29.29.29.29
```

```
LSP ID: 1                      Tunnel ID: 1
Upstream Label: 3
Token bucket rate: 0.00        Token bucket size: 0.00
```

Table 400 Description on the fields of display mpls rsvp-te reservation

Field	Description
Interface Ethernet1/0	RSVP-TE enabled Ethernet interface
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
LSP ID	LSP ID
Tunnel ID	Tunnel ID
Upstream Label	Upstream label
Token Bucket rate	Token bucket rate, a traffic parameter
Token Bucket Size	Token bucket size, a traffic parameter

display mpls rsvp-te rsb-content

Syntax **display mpls rsvp-te rsb-content** { *ingress-lsr-id Ispid tunnel-id egress-lsr-id nexthop-address* } [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter *ingress-lsr-id*: Ingress LSR ID.

lspid: Local LSP ID, in the range 1 to 65,535.

tunnel-id: Tunnel ID, in the range 0 to 65,535.

egress-lsr-id: Egress LSR ID.

nexthop-address: Next hop address.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te rsb-content** command to display information about RSVP-TE reservation state blocks (RSBs).

Example # Display information about RSVP-TE RSBs.

```
<Sysname> display mpls rsvp-te rsb-content 19.19.19.19 1 0 29.29.29.29 101.1
01.101.2
The RSB Content:
```

```
Tunnel Dest: 29.29.29.29    Session Tunnel ID: 0
Tunnel ExtID: 19.19.19.19
Next Hop: 101.101.101.2    Resevation Style: SE Style
Reservation Incoming Interface: Ethernet1/0
Reservation Interface: Ethernet1/0
Message ID : 2
Filter Spec Information-
  The filter number: 1
  Ingress LSR ID: 19.19.19.19    Local LSP ID: 1      OutLabel: 3
  Graceful Restart State: Stale
RRO Information-
RRO-Flag is
  RRO-CType: IPV4   RRO-IPAddress: 101.101.101.2      RRO-IPPrefixLen: 32
FlowSpec Information-
  Token bucket rate: 2500.00
  Token bucket size: 0.00
  Peak data rate: 0.00
  Minimum policed unit: 0
  Maximum packet size: 0
  Bandwidth guarantees: 0.00
  Delay guarantees: 0
  Qos Service is Controlled
Resv Message arrive on Ethernet1/0 from NHOP 101.101.101.2
Graceful Restart State: Stale
```

Table 401 Description on the fields of display mpls rsvp-te rsb content

Field	Description
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Session Tunnel ID	Session tunnel ID
Tunnel Ext ID	Tunnel extension (ingress LSR ID), in the format of X.X.X.X
Next Hop	Next hop address, in the format of X.X.X.X
Reservation Style	Reservation style: SE or FF
Reservation Interface	Reservation interface name
Reserve Incoming Interface	Incoming interface where the Resv message was received
Message ID	Message ID of the Refresh Reduction message
Filter Spec Information	Filter specifications
The filter number	Number of filters
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
LSP ID	LSP ID
Out Label	Outgoing label
RRO Information	Information about route recording
RRO-C Type	Type of route recording
RRO-IP Address	IP address of recorded route in the format of X.X.X.X
RRO-IPPrefixLen	IP prefix length of recorded route
Flow Spec information	Flow specifications
Token Bucket rate	Token bucket rate (in kbps), a traffic parameter
Token Bucket size	Token bucket size, a traffic parameter
Peak Data Rate	Peak data rate (in kbps), a traffic parameter
Maximum packet size	Maximum packet size, a traffic parameter
Minimum policed unit	Minimum policed unit, a traffic parameter
Bandwidth guarantees	Guaranteed bandwidth, a reservation specifications parameter
Delay guarantees	Delay guarantee, a reservation specifications parameter

Table 401 Description on the fields of display mpls rsvp-te rsb content

Field	Description
QOS service	QoS guarantee/control
Resv Message	Reservation message received on a particular interface from next hop (X.X.X.X)
Graceful Restart State	State of GR: stale or normal. Displayed as --- when not supported by the device.

display mpls rsvp-te sender

Syntax **display mpls rsvp-te sender** [**interface** *interface-type interface-number*] [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and number.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls rsvp-te sender** command to display RSVP-TE sender message information.

Example # Display the RSVP-TE sender message information on interface Ethernet 1/0.

```
<Sysname> display mpls rsvp-te sender interface ethernet 1/0
Interface Ethernet1/0;
 Tunnel Dest: 29.29.29.29    Ingress LSR ID: 19.19.19.19
 LSP ID: 1                   Session Tunnel ID: 1
 Session Name: Tunnel0
 Previous Hop Address: 101.101.101.1
 Token bucket rate: 0.0      Token bucket size: 0.00
```

Display the RSVP-TE sender message information on all interfaces.

```
<Sysname> display mpls rsvp-te sender
Interface: Ethernet1/0
 Tunnel Dest: 19.19.19.19    Ingress LSR ID: 29.29.29.29
 LSP ID: 1                   Session Tunnel ID: 0
 Session Name: Tunnel0
 Previous Hop Address: 101.101.101.2
 Token bucket rate: 0.0      Token bucket size: 0.00
Interface: Incoming-Interface at the Ingress
```

```
Tunnel Dest: 29.29.29.29    Ingress LSR ID: 19.19.19.19
LSP ID: 1                   Session Tunnel ID: 0
Session Name: Tunnel1
Previous Hop Address: 19.19.19.19
Token bucket rate: 0.0      Token bucket size: 0.00
```

Table 402 Description on fields of the display mpls rsvp-te sender command

Field	Description
Interface Ethernet1/0	RSVP-TE enabled Ethernet interface
Tunnel Dest	Tunnel destination, in the format of X.X.X.X
Ingress LSR ID	Ingress LSR ID, in the format of X.X.X.X
LSP ID	LSP ID
Tunnel ID	Tunnel ID
Session Name:	Session name
Previous Hop Address	Previous hop address, in the format of X.X.X.X
Token Bucket rate	Token bucket rate, a traffic parameter
Token Bucket Size	Token bucket size, a traffic parameter

display mpls rsvp-te statistics

Syntax **display mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*] }

View Any view

Parameter **global**: Display global RSVP-TE information.

interface: Displays statistics about RSVP-TE for a specified or all interfaces if no interface is specified.

interface-type interface-number: Specifies an interface for which statistics about RSVP-TE is displayed.

Description Use the **display mpls rsvp-te statistics** command to display statistics about RSVP-TE.

Example # Display global RSVP-TE statistics.

```
<Sysname> display mpls rsvp-te statistics global
LSR ID: 1.1.1.1
 PSB Count: 1                          RSB Count: 1
 RFSB Count: 0                         TCSB Count: 1
 LSP Count: 1

Total Statistics Information:
 PSB CleanupTimeOutCounter: 0          RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 55                 RecPacketCounter: 54
 SendPathCounter: 5                    RecPathCounter: 0
 SendResvCounter: 0                    RecResvCounter: 4
 SendResvConfCounter: 0                RecResvConfCounter: 0
 SendHelloCounter: 2                   RecHelloCounter: 48
```

```
 SendAckCounter: 48                    RecAckCounter: 2
 SendPathErrCounter: 0                 RecPathErrCounter: 0
 SendResvErrCounter: 0                 RecResvErrCounter: 0
 SendPathTearCounter: 0                RecPathTearCounter: 0
 SendResvTearCounter: 0                RecResvTearCounter: 0
 SendSrefreshCounter: 0                RecSrefreshCounter: 0
 SendAckMsgCounter: 0                  RecAckMsgCounter: 0
 SendErrMsgCounter: 0                  RecErrMsgCounter: 0
 RecReqFaultCounter: 0
```

Display the RSVP-TE statistics of interface Serial 1/0.

```
<Sysname> display mpls rsvp-te statistics interface
Serial1/0:
 PSB CleanupTimeOutCounter: 0          RSB CleanupTimeOutCounter: 0
 SendPacketCounter: 69                 RecPacketCounter: 68
 SendPathCounter: 6                    RecPathCounter: 0
 SendResvCounter: 0                    RecResvCounter: 5
 SendResvConfCounter: 0                RecResvConfCounter: 0
 SendHelloCounter: 2                   RecHelloCounter: 61
 SendAckCounter: 61                    RecAckCounter: 2
 SendPathErrCounter: 0                 RecPathErrCounter: 0
 SendResvErrCounter: 0                 RecResvErrCounter: 0
 SendPathTearCounter: 0                RecPathTearCounter: 0
 SendResvTearCounter: 0                RecResvTearCounter: 0
 SendSrefreshCounter: 0                RecSrefreshCounter: 0
 SendAckMsgCounter: 0                  RecAckMsgCounter: 0
 SendErrMsgCounter: 0                  RecErrMsgCounter: 0
 RecReqFaultCounter: 0
```

Table 403 Description on the fields of the display mpls rsvp-te statistics command

Field	Description
LSR ID	LSR ID
PSB Count	Number of PSBs
RSB Count	Number of RSBs
RFSB Count	Number of RFSBs
TCSB Count	Number of TCSBs
LSP Count	Number of LSPs
PSB CleanupTimeOutCounter	Number of PSB timeouts
RSB CleanupTimeOutCounter	Number of RSB timeouts
SendPacketCounter	Number of transmitted packets
RecPacketCounter	Number of received packets
SendPathCounter	Number of transmitted Path messages
RecPathCounter	Number of received Path messages
SendResvCounter	Number of transmitted Resv messages
RecResvCounter	Number of received Resv messages
SendResvConfCounter	Number of transmitted ResvConf messages
RecResvConfCounter	Number of received ResvConf messages
SendHelloCounter	Number of transmitted Hello messages
RecHelloCounter	Number of received Hello messages
SendAckCounter	Number of transmitted Ack messages

Table 403 Description on the fields of the display mpls rsvp-te statistics command

Field	Description
RecAckCounter	Number of received Ack messages
SendPathErrCounter	Number of transmitted PathErr messages
RecPathErrCounter	Number of received PathErr messages
SendResvErrCounter	Number of transmitted ResvErr messages
RecResvErrCounter	Number of received ResvErr messages
SendPathTearCounter	Number of transmitted PathTear messages
RecPathTearCounter	Number of received PathTear messages
SendResvTearCounter	Number of transmitted ResvTear messages
RecResvTearCounter	Number of received ResvTear messages
SendSrefreshCounter	Number of transmitted Srefresh messages
RecSrefreshCounter	Number of received Srefresh messages
SendAckMsgCounter	Number of transmitted AckMsg messages
RecAckMsgCounter	Number of received AckMsg messages
SendErrMsgCounter	Number of transmitted errors
RecErrMsgCounter	Number of received errors
RecReqFaultCounter	Number of request failures

display mpls static-cr-lsp

Syntax **display mpls static-cr-lsp** [**lsp-name** *lsp-name*] [{ **exclude** | **include** } *ip-address prefix-length*] [**verbose**]

View Any view

Parameter **lsp-name** *lsp-name*: Label switched path name comprising 1 to 15 characters.

exclude: Displays only CR-LSPs with destination IP addresses other than the one specified by the *ip-address prefix-length* arguments.

include: Displays only CR-LSPs with the destination IP address specified by the *ip-address prefix-length* arguments.

ip-address: Destination IP address.

prefix-length: IP address prefix length, in the range 0 to 32.

verbose: Displays detailed information.

Description Use the **display mpls static-cr-lsp** command to display information about static CR-LSPs.

Example # Display brief information about all static CR-LSPs.

```
<Sysname> display mpls static-cr-lsp
total statics-cr-lsp : 1
```

```
Name        FEC                I/O Label   I/O If                Stat
Tunnel0     3.3.3.9/32         NULL/100    -/Eth1/0              Down
```

Table 404 Description on the fields of the display mpls static-cr-lsp command

Field	Description
Name	Static CR-LSP name
FEC	Forwarding equivalence class (FEC) associated with the destination IP address of LSP
I/O Label	Incoming/outgoing label
I/O If	Incoming/outgoing interface
Stat	Current state of the CR-LSP

Display detailed information about all static CR-LSPs.

```
<Sysname> display mpls static-cr-lsp verbose
No             : 1
LSP-Name       : Tunnel0
LSR-Type       : Transit
FEC            : -/-
In-Label       : 20
Out-Label      : 30
Ingress LsrId  : 34.1.1.1
Tunnel Id      : 2
In-Interface   : Ethernet1/0
Out-Interface  : Ethernet1/1
NextHop        : 3.2.1.2
```

Table 405 Description on the fields of display mpls static-cr-lsp verbose

Field	Description
LSP-Name	Static CR-LSP name
LSR-Type	LSR type: ingress, transit, or egress
FEC	Forwarding equivalence class (FEC)
In-Label	Incoming label
Out-Label	Outgoing label
Ingress LsrId	Ingress LSR ID
Tunnel Id	Tunnel ID
In-Interface	Incoming interface
Out-Interface	Outgoing interface
NextHop	Next hop address

display mpls te cspf tedb

Syntax **display mpls te cspf tedb** { **all** | **area** *area-id* | **interface** *ip-address* | **network-lsa** | **node** [*mpls-lsr-id*] } [| { **begin** | **include** | **exclude** } *regular-expression*]

View Any view

Parameter *area-id*: Area ID. For OSPF, it ranges from 0 to 4294967295; for IS-IS, it takes the value of 1 or 2.

ip-address: IP address of an interface.

network-lsa: Displays traffic engineering database (TEDB) information in network LSAs.

node: Displays the TEDB information on nodes. If no node is specified, the TEDB information on all nodes is displayed.

mpls-lsr-id: Specifies a node by its MPLS LSR ID.

|: Filters output by regular expression.

begin: Displays information beginning with a defined regular expression.

include: Displays information that includes a defined regular expression.

exclude: Displays information that excludes a defined regular expression.

regular-expression: Regular expression, a string of 1 to 80 characters without spaces.

Description Use the **display mpls te cspf tedb** command to display information about CSPF-based TEDB by specified criteria.

Example # Display TEDB information in network LSAs.

```
<Sysname> display mpls te cspf tedb network-lsa
Maximum Network LSA Supported:  500
Current Total Network LSA Number:       7
Id   DR MPLS LSR-Id DR-Address       IGP   Process-Id  Area  Neighbor
1    8.1.1.2        3.0.0.2          OSPF  100         0     1.1.1.1
                                                             2.1.1.1
                                                             8.1.1.2
2    2.1.1.1        3.0.0.3          OSPF  100         0     2.1.1.1
                                                             3.1.1.1
                                                             2.1.1.2
3    3.1.1.2        3.0.0.4          OSPF  100         0     3.1.1.1
                                                             4.1.1.1
                                                             3.1.1.2
4    4.1.1.2        3.0.0.5          OSPF  100         0     4.1.1.1
                                                             5.1.1.1
                                                             4.1.1.2
5    5.1.1.2        3.0.0.6          OSPF  100         0     5.1.1.1
                                                             6.1.1.1
                                                             5.1.1.2
6    6.1.1.2        3.0.0.9          OSPF  100         0     6.1.1.1
                                                             7.1.1.1
                                                             6.1.1.2
7    7.1.1.1        12.0.0.7         OSPF  100         0     3.1.1.1
                                                             7.1.1.1
                                                             7.1.1.2
```

Table 406 Description on the fields of the display mpls te cspf tedb command

Field	Description
ID	Number
DR MPLS LSR-Id	MPLS LSR ID of the designated router (DR)
DR-Address	Interface address of the DR
IGP	Interior gateway protocol: OSPF or IS-IS

Table 406 Description on the fields of the display mpls te cspf tedb command

Field	Description
Process-Id	IGP process ID
Area	Area to which the router belongs
Neighbor	Neighbor router ID

Display all TEDB information.

```
<Sysname> display mpls te cspf tedb all
Maximum Node Supported: 1000            Maximum Link Supported: 4000
Current Total Node Number: 3            Current Total Link Number: 44
Id    MPLS LSR-Id     IGP     Process-Id    Area            Link-Count
1     1.1.1.1         OSPF    100           1001,1002,1003  20
                                            1004,1005,1006
                                            1007,1008,1009
                                            1010,1,2
                                            13,14,15
                                            16,17,18
                                            19,20
2     2.1.1.1         ISIS    100           Level-0,1       20
3     3.1.1.1         OSPF    100           0               4
```

Table 407 Description on the fields of the display mpls te cspf tedb all command

Field	Description
ID	Number
MPLS LSR-Id	MPLS LSR ID
IGP	Interior gateway protocol: OSPF or IS-IS
Process-Id	IGP process ID
Area	Area to which the router belongs
Link-count	Total number of connected links belonging to a particular IGP protocol process

Display the TEDB information of IGP area 1.

```
<Sysname> display mpls te cspf tedb area 1
Router Node Information for Area 1:
Id     MPLS LSR-Id    IGP     Process-Id     Area            Link-Count
1      2.2.2.2        OSPF    100            1               1
2      3.3.3.3        OSPF    100            1               1
3      2.2.2.2        ISIS    100            Level-1         1
4      3.3.3.3        ISIS    100            Level-1         1

Network LSA Information for Area 1:
Id   DR MPLS LSR-Id  DR-Address    IGP  Process-Id Area    Neighbor
1    3.3.3.3         20.1.1.2      OSPF 100        1       2.2.2.2
                                                           3.3.3.3
2    3.3.3.3         20.1.1.2      ISIS 100        Level-1 3.3.3.3
                                                           2.2.2.2
```

Table 408 Description on the fields of the display mpls te cspf tedb area command

Field	Description
Id	Number
MPLS LSR-Id	MPLS LSR ID, in dotted decimal notation
IGP	Interior gateway protocol: OSPF or IS-IS
Process-Id	IGP process ID
Area	Area to which the router belongs

Table 408 Description on the fields of the display mpls te cspf tedb area command

Field	Description
Link-Count	Total number of connected links belonging to a particular IGP protocol process
DR MPLS LSR-Id	MPLS LSR ID of the DR
DR-Address	Interface address of the DR
Neighbor	MPLS LSR ID of the neighbor

Display the TEDB information of all nodes.

```
<Sysname> display mpls te cspf tedb node
MPLS LSR-Id: 1.1.1.1
  IGP Type: OSPF   Process Id: 100
  MPLS-TE Link Count: 1
  Link[1] :
    Interface IP Address: 2.0.0.33, 2.0.0.35, 2.0.0.36,
    Neighbor  IP Address: 2.0.0.2, 2.0.0.42, 2.0.0.43,
                          2.0.0.44, 2.0.0.45, 2.0.0.46,
                          2.0.0.47, 2.0.0.32,
    Neighbor  MPLS LSR-Id : 1.1.1.2
    IGP Area: 1
    Link  Type: point-to-point  Link Status: Inactive
    IGP Metric: 100             TE Metric: 100         Color: 0xff
    Maximum Bandwidth: 100 (kbps)
    Maximum Reservable Bandwidth: 20 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0] :  100        (kbps)   LOM[0] :  1
         BC[1] :  20         (kbps)   LOM[1] :  1
    BW Unreserved for Class type 0:
         [0] :    10         (kbps),  [1] :     10         (kbps)
         [2] :    10         (kbps),  [3] :     10         (kbps)
         [4] :    10         (kbps),  [5] :     10         (kbps)
         [6] :    10         (kbps),  [7] :     10         (kbps)
    BW Unreserved for Class type 1:
         [0] :    10         (kbps),  [1] :     10         (kbps)
         [2] :    10         (kbps),  [3] :     10         (kbps)
         [4] :    10         (kbps),  [5] :     10         (kbps)
         [6] :    10         (kbps),  [7] :     10         (kbps)
MPLS LSR-Id: 1.1.1.1
  IGP Type: ISIS   Process Id: 100
  MPLS-TE Link Count: 2
  Link[1] :
    Interface IP Address: 2.0.0.33, 2.0.0.35, 2.0.0.36,
    Neighbor  IP Address: 2.0.0.2, 2.0.0.42, 2.0.0.43,
                          2.0.0.44, 2.0.0.45, 2.0.0.46,
                          2.0.0.47, 2.0.0.32, 2.0.0.33
    Neighbor  MPLS LSR-Id: 1.1.1.2
    IGP Area: Level-0
    Link  Type: point-to-point  Link Status: Active
    IGP Metric: 10              TE Metric: 10          Color: 0x11
    Maximum Bandwidth: 100 (kbps)
    Maximum Reservable Bandwidth: 100 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0] :  100        (kbps)   LOM[0] :  1
         BC[1] :  20         (kbps)   LOM[1] :  1
    BW Unreserved for Class type 0:
```

```
          [0] :    10          (kbps),  [1] :     10          (kbps)
          [2] :    10          (kbps),  [3] :     10          (kbps)
          [4] :    10          (kbps),  [5] :     10          (kbps)
          [6] :    10          (kbps),  [7] :     10          (kbps)
    BW Unreserved for Class type 1:
          [0] :    10          (kbps),  [1] :     10          (kbps)
          [2] :    10          (kbps),  [3] :     10          (kbps)
          [4] :    10          (kbps),  [5] :     10          (kbps)
          [6] :    10          (kbps),  [7] :     10          (kbps)
```

Table 409 Description on the fields of the display mpls te cspf tedb node command

Field	Description
MPLS LSR-Id	MPLS LSR ID of node
IGP_Type	IGP type
Process Id	IGP process ID
MPLS-TE Link Count	Number of MPLS TE links
Link[x]	Specific link, with the bracketed x indicating the link number
Interface IP Address	Interface IP address
DR Address	IP address of the DR
IGP Area	IGP area
Link Type	Link type
Link Status	Link status
IGP Metric	IGP metric of link
TE Metric	TE metric of link
Color	Link administrative attribute
Maximum Bandwidth	Maximum link bandwidth
Maximum Reservable Bandwidth	Maximum reservable bandwidth of link
Bandwidth Constraints	Bandwidth constraints
BW Unreserved for Class type0	Unreserved bandwidth at the CT0 level
BW Unreserved for Class type1	Unreserved bandwidth at the CT1 level

Display TEDB information for a specified interface address.

```
<Sysname> display mpls te cspf tedb interface 20.1.1.1
MPLS LSR-Id: 2.2.2.2
  IGP Type: ISIS   Process Id: 100
  Link[1] :
    Interface IP Address: 20.1.1.1
    DR Address: 20.1.1.2
    IGP Area: Level-1
    Link  Type: multi-access  Link Status: Active
    IGP Metric: 10              TE Metric: 0           Color: 0x0
    Maximum Bandwidth: 0 (kbps)
    Maximum Reservable Bandwidth: 0 (kbps)
    Bandwidth Constraints:           Local Overbooking Multiplier:
         BC[0] :  0          (kbps)   LOM[0] :  1
         BC[1] :  0          (kbps)   LOM[1] :  1
    BW Unreserved for Class type 0:
         [0] :    0          (kbps),  [1] :     0          (kbps)
         [2] :    0          (kbps),  [3] :     0          (kbps)
         [4] :    0          (kbps),  [5] :     0          (kbps)
```

```
      [6] :    0          (kbps),  [7] :     0          (kbps)
  BW Unreserved for Class type 1:
      [0] :    0          (kbps),  [1] :     0          (kbps)
      [2] :    0          (kbps),  [3] :     0          (kbps)
      [4] :    0          (kbps),  [5] :     0          (kbps)
      [6] :    0          (kbps),  [7] :     0          (kbps)
```

Table 410 Description on the fields of display mpls te cspf tedb interface

Field	Description
MPLS LSR-Id	MPLS LSR ID of node
IGP_Type	IGP type
Process Id	IGP process ID
MPLS-TE Link Count	Number of MPLS TE links
Link[x]	Specific link, with the bracketed x indicating the link number
Interface IP Address	Interface IP address
DR Address	IP address of the DR
IGP Area	IGP area
Link Type	Link type
Link Status	Link status
IGP Metric	IGP metric of link
TE Metric	TE metric of link
Color	Link administrative attribute
Maximum Bandwidth	Maximum link bandwidth
Maximum Reservable Bandwidth	Maximum reservable bandwidth of link
Bandwidth Constraints	Bandwidth constraints
BW Unreserved for Class type0	Unreserved bandwidth at the CT0 level
BW Unreserved for Class type1	Unreserved bandwidth at the CT1 level

display mpls te link-administration admission-control

Syntax **display mpls te link-administration admission-control** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and a number.

Description Use the **display mpls te link-administration admission-control** command to display information about CR-LSPs carried on the link of a specified interface or links of all interfaces if no interface is specified.

Example # Display information about the CR-LSPs carried on the links of all interfaces.

```
<Sysname> display mpls te link-administration admission-control
LspID           In/Out IF         S/H Prio    CT       BW(kbps)
```

```
1.1.1.9:1024     ---/Eth1/0        7/7          0         0
1.1.1.9:2048     ---/Eth1/1        7/7          0         0
```

Table 411 Description on fields of the command

Field	Description
LspID	ID of an LSP carried on a link
In/Out IF	Incoming/Outgoing interface
S/H Prio	Setup and holding priorities of CR-LSP
CT	Service class type
BW(kbps)	Bandwidth (in kbps)

display mpls te link-administration bandwidth-allocation

Syntax **display mpls te link-administration bandwidth-allocation** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by its type and a number.

Description Use the **display mpls te link-administration bandwidth-allocation** command to display bandwidth allocation on the specified or all MPLS TE enabled interfaces.

Example # Display bandwidth allocation on MPLS TE enabled interfaces.

```
<Sysname> display mpls te link-administration bandwidth-allocation
  Link ID                    :  Ethernet1/0
  Physical Bandwidth Type0   :  0 kbits/sec
  Physical Bandwidth Type1   :  0 kbits/sec
  Reservable Bandwidth Type0 :  0 kbits/sec
  Reservable Bandwidth Type1 :  0 kbits/sec
  Downstream LSP Count       :  0
  UpStream LSP Count         :  0
  Downstream Bandwidth       :  0 kbits/sec
  Upstream Bandwidth         :  0 kbits/sec
  IPUpdown Link Status       :  UP
  PhysicalUpdown Link Status :  UP
  TE CLASS    CLASS TYPE    PRIORITY     BW RESERVED    BW AVAILABLE
      0           0             0            0             0
      1           0             1            0             0
      2           0             2            0             0
      3           0             3            0             0
      4           0             4            0             0
      5           0             5            0             0
      6           0             6            0             0
      7           0             7            0             0
      8           1             0            0             0
      9           1             1            0             0
     10           1             2            0             0
     11           1             3            0             0
```

```
12              1               4               0               0
13              1               5               0               0
14              1               6               0               0
15              1               7               0               0
```

Table 412 Description on the fields of the command

Field	Description
Link ID	Link ID
Physical Bandwidth Type0	CT0 physical bandwidth
Physical Bandwidth Type1	CT1 physical bandwidth
Reservable Bandwidth Type0	CT0 reservable bandwidth
Reservable Bandwidth Type1	CT1 reservable bandwidth
Downstream LSP Count	Number of downstream LSPs
UpStream LSP Count	Number of upstream LSPs
IPUpdown Link Status	IP layer link status
PhysicalUpdown Link Status	Physical layer link status
TE CLASS	TE class
CLASS TYPE	Service class type
PRIORITY	Priority
BW RESERVED	Reserved bandwidth

display mpls te tunnel

Syntax **display mpls te tunnel** [**destination** *dest-addr*] [**lsp-id** *lsr-id lsp-id*] [**lsr-role** { **all** | **egress** | **ingress** | **remote** | **transit** }] [**name** *name*] [{ **incoming-interface** | **outgoing-interface** | **interface** } *interface-type interface-number*] [**verbose**]

View Any view

Parameter **destination** *address*: Specifies a destination IP address to display only the tunnels with the specified destination IP address.

lsr-id: LSR ID of the ingress node, in dotted decimal notation.

lsp-id: LSP ID, in the range 1 to 65535.

lsr-role: Displays tunnels by LSR role (ingress, transit, egress, or remote).

all: Displays all tunnels.

ingress: Displays tunnels created taking current device as the ingress.

transit: Displays tunnels created taking current device as a transit node.

egress: Displays tunnels created taking current device as the egress.

name *name*: Displays the tunnel with a particular name. This could be a string of 1 to 63 characters configured as interface description or the interface name if no interface description is configured. The tunnel name should be signaled to all hops.

incoming-interface: Displays all tunnels that use the interface identified by the *interface-type interface-number* arguments as the incoming interface.

outgoing-interface: Displays all tunnels that use the interface identified by the *interface-type interface-number* arguments as the outgoing interface.

interface: Displays all tunnels that use the interface identified by the *interface-type interface-number* arguments as the incoming or outgoing interface.

interface-type interface-number: Specifies an interface by its type and number.

verbose: Displays detailed information.

Description

Use the **display mpls te tunnel** command to display information about MPLS TE tunnels.

Example

Display information about MPLS TE tunnels. (The output may vary by signaling protocol.)

```
<Sysname> display mpls te tunnel
LSP-Id            Destination     In/Out-If            Name
1.1.1.9:1024      3.3.3.9         -/Eth1/0             Tunnel0
1.1.1.9:2048      3.3.3.9         -/Eth1/1             Tunnel0
```

Table 413 Description on the fields of the display mpls te tunnel command

Field	Description
LSP-ID	LSP ID of tunnel
Destination	Destination router ID
In/Out-IF	Incoming/outgoing interface
Name	Tunnel name configured on the ingress node

Display detailed information about MPLS TE tunnels.

```
<Sysname> display mpls te tunnel verbose
No             : 1
LSP-Id         : 1.1.1.9:1024
Tunnel-Name    : Tunnel0
Destination    : 3.3.3.9
In-Interface   : -
Out-Interface  : Eth1/0
Tunnel BW      : 0 kbps
Class Type     : bc0
Ingress LSR-Id : 1.1.1.9
Egress LSR-Id  : 3.3.3.9
Setup-Priority : 7
Hold-Priority  : 7
Sign-Protocol  : RSVP TE
Resv Style     : SE
IncludeAnyAff  : 0x0
ExcludeAllAff  : 0x0
IncludeAllAff  : 0x0
Created Time   : 2004/10/18 16:05:17
```

Table 414 Description on the fields of the display mpls te tunnel verbose command

Field	Description
No	Number
LSP-Id	LSP ID of tunnel
Tunnel-Name	Tunnel name configured on the ingress node
Destination	Destination router ID
In-Interface	Incoming interface
Out-Interface	Outgoing interface
Tunnel BW	Tunnel bandwidth
Class Type	Service class type
Ingress LSR-Id	Ingress LSR ID
Setup-Priority	Setup priority of link
Hold-Priority	Holding priority of link
Sign-Protocol	Signaling protocol
Resv Style	Reservation style
IncludeAnyAff	Any affinity properties that must be included
ExcludeAllAff	Link properties that are excluded
IncludeAllAff	All link affinity properties that must be included
Created Time	Time when the tunnel was created

display mpls te tunnel path

Syntax **display mpls te tunnel path** [**tunnel-name** *tunnel-name*] [**lsp-id** *lsr-id lsp-id*]

View Any view

Parameter **tunnel-name** *tunnel-name*: Tunnel name, a string of 1 to 63 characters.

lsr-id: Ingress LSR ID, in dotted decimal notation.

lsp-id: LSP ID, in the range 1 to 65535.

Description Use the **display mpls te tunnel path** command to display the path or paths that the specified or all MPLS TE tunnels traverse on this node.

Example # Display the paths that all MPLS TE tunnels traverse.

```
<Sysname> display mpls te tunnel path
Tunnel Interface Name Tunnel0:
Lsp ID :  1.1.1.9:10
Hop information:
Hop 0: 192.1.1.1;
Hop 1: 12.1.1.2;
Hop 2: 10.202.2.2.
```

Table 415 Description on the fields of the display mpls te tunnel path command

Field	Description
Tunnel Interface Name Tunnel0	Tunnel interface name, Tunnel0 in this sample output
Lsp ID	LSP ID
Hop 0	Hop 0 on the path
Hop 1	Hop 1 on the path
Hop 2	Hop 2 on the path

display mpls te tunnel statistics

Syntax **display mpls te tunnel statistics**

View Any view

Parameter None

Description Use the **display mpls te tunnel statistics** command to display statistics about MPLS TE tunnels.

Example # Display statistics about MPLS TE tunnels.

```
<Sysname> display mpls te tunnel statistics
Ingress:   0 Tunnels,   0 Up,   0 Modified,   0 In-Progress,   0 Failed
Transit:   0 Up
Egress :   0 Up
```

Table 416 Description on the fields of display mpls te tunnel statistics

Field	Description
Ingress	This device is the tunnel ingress.
Transit	This device is a transit node on the tunnel.
Egress	This device is the tunnel egress.

display mpls te tunnel-interface

Syntax **display mpls te tunnel-interface**

View Any view

Parameter None

Description Use the **display mpls te tunnel-interface** command to display information about MPLS TE tunnel interfaces on this node.

Example # Display information about MPLS TE tunnel interfaces on this node.

```
<Sysname> display mpls te tunnel-interface
  Tunnel Name         :  Tunnel0
```

```
Tunnel Desc         :  Tunnel Interface
Tunnel State Desc   :  CR-LSP is Up
Tunnel Attributes   :
  LSP ID              :  1.1.1.9:1
  Session ID          :  0
  Admin State         :  UP                    Oper State   :  UP
  Ingress LSR ID      :  1.1.1.9               Egress LSR ID:  2.2.2.9
  Signaling Prot      :  STATIC-CR             Resv Style   :  -
  Class Type          :  CLASS 0               Tunnel BW    :  0
  Setup Priority      :  7                     Hold Priority:  7
  Affinity Prop/Mask  :  0/0
  Explicit Path Name  :  -
  Tie-Breaking Policy :  None
  Metric Type         :  None
  Record Route        :  Disabled              Record Label :  Disabled
  FRR Flag            :  Disabled          BackUpBW Flag:  Not Supported
  BackUpBW Type       :  -                     BackUpBW     :  -
  Route Pinning       :  Disabled
  Retry Limit         :  5                     Retry Interval:  10
  Reopt               :  Disabled              Reopt Freq   :  -
  Back Up Type        :  None
  Back Up LSPID       :  -
  Auto BW             :  Disabled              Auto BW Freq :  -
  Min BW              :  -                     Max BW       :  -
  Current Collected BW:  -
      Interfaces Protected:  -
  VPN Bind Type       :  NONE
  VPN Bind Value      :  -
  Car Policy          :  Disabled
```

Table 417 Description on the fields of display mpls te tunnel-interface command

Field	Description
Tunnel Name	Tunnel name
Tunnel Desc	Tunnel description
Tunnel State Desc	Tunnel state description
LSP ID	LSP ID
Session ID	Session ID
Admin State	Administrative state
Oper State	Operation state
Ingress LSR ID	Ingress LSR ID
Egress LSR ID	Egress LSR ID
Signaling Prot	Signaling protocol
Resv Style	Reservation style
Class Type	Service class type
Tunnel BW	Tunnel bandwidth
Setup Priority	Setup priority of LSP
Hold Priority	Hold priority of LSP
Affinity Prop/Mask	Affinity attribute and mask
Explicit Path Name	Explicit path name
Tie-Breaking Policy	Path selection policy
Metric Type	Metric type
Record Route	State of the route recording function
Record Label	State of the label recording function
FRR Flag	Fast reroute (FRR) flag

Table 417 Description on the fields of display mpls te tunnel-interface command

Field	Description
BackUpBW Flag	Backup bandwidth flag
BackUpBW Type	Backup bandwidth type
BackUpBW	Backup bandwidth
Route Pinning	Route pinning function
Retry Limit	Maximum number of setup retries
Retry Interval	Retry interval
Reopt	State of the reoptimization function
Reopt Freq	Reoptimization interval
Back Up Type	Backup path type
Back Up LSPID	Backup LSP ID
Auto BW	State of the automatic bandwidth adjustment function
Auto BW Freq	Automatic bandwidth adjustment interval
Min BW	Lower limit for automatic bandwidth adjustment
Max BW	Upper limit for automatic bandwidth adjustment
Current Collected BW	Bandwidth information currently collected
Interfaces Protected	FRR protected interfaces
VPN Bind Type	Type of the binding, VPN or ACL
VPN Bind Value	Value of the binding, the VPN instance name or ACL number
Car Policy	Whether CAR policy is enabled

display ospf mpls-te

Syntax **display ospf** [*process-id*] **mpls-te** [**area** *area-id*] [**self-originated**]

View Any view

Parameter *process-id*: OSPF process ID, in the range 1 to 65535. If a process is specified, only the TE LSAs of this process are displayed; if no process is specified, the TE LSAs of all processes are displayed.

area *area-id*: Displays the TE LSAs of a specified OSPF area. The *area-id* argument takes an integer in the range 0 to 4294967295 or the form of IPv4 address.

self-originated: Displays self originated TE LSAs.

Description Use the **display ospf mpls-te** command to display TE LSAs in the link state database (LSDB).

Example # Display all TE LSAs in the LSDB.

```
<Sysname> display ospf mpls-te
OSPF Process 100 with Router ID 10.0.0.1
Area ID:
 Traffic Engineering LSA's of the database
-------------------------------------------------
```

```
LSA []
-----------------------------------------------
  LSA  Type                  : Opq-Area
  Opaque Type               : 1
  Opaque ID                 :
  Advertising Router ID  : xxx.xxx.xxx.xxx
  LSA  Age                  :
  Length                    :
  LSA  Options              :
  LS Seq Number             :
  CheckSum                  :

  Link Type               :Point to Point / Point to Multi Point /MultiAccess
  Link ID                   :
  Local Interface Address  : xxx.xxx.xxx.xxx
  Remote Interface Address : xxx.xxx.xxx.xxx
  TE Metric                 :
  Maximum Bandwidth         :  bytes/sec
  Maximum Reservable BW     :  bytes/sec
  Admin Group               :

  Global Pool:
      Unreserved BW [ 0] =   0  bytes/sec
      Unreserved BW [ 1] =   0  bytes/sec
      Unreserved BW [ 2] =   0  bytes/sec
      Unreserved BW [ 3] =   0  bytes/sec
      Unreserved BW [ 4] =   0  bytes/sec
      Unreserved BW [ 5] =   0  bytes/sec
      Unreserved BW [ 6] =   0  bytes/sec
      Unreserved BW [ 7] =   0  bytes/sec
  Sub Pool :
      Unreserved BW [ 0] =   0  bytes/sec
      Unreserved BW [ 1] =   0  bytes/sec
      Unreserved BW [ 2] =   0  bytes/sec
      Unreserved BW [ 3] =   0  bytes/sec
      Unreserved BW [ 4] =   0  bytes/sec
      Unreserved BW [ 5] =   0  bytes/sec
      Unreserved BW [ 6] =   0  bytes/sec
      Unreserved BW [ 7] =   0  bytes/sec

  Bandwidth Constraints:
      BC [ 0] =   bytes/sec  BC [ 1] =    bytes/sec

  Local OverBooking Multipliers:
      LOM [ 0] =   1     LOM [ 1] =   1
```

Table 418 Description on the fields of the display ospf mpls-te command

Field	Description
Area ID	TE enabled OSPF area ID.
LSA Type	LSA type which must be Opd-Area, carried in the Opaque LSA header
Opaque Type	1 for TE, carried in the header of Opaque LSA
Opaque ID	Opaque ID, carried in the header of Opaque LSA
Advertising Router ID	Router ID of the node where the LSA was generated
LSA age	LSA age, carried in the header of Opaque LSA
Length	LSA length, carried in the header of Opaque LSA
LSA Options	LSA options, carried in the header of Opaque LSA
LS Seq Number	LSA sequence number, carried in the header of Opaque LSA
Checksum	LSA checksum, carried in the header of Opaque LSA
Link Type	Link type: point to point, point to multipoint, or multiAccess
Link ID	Link ID

Table 418 Description on the fields of the display ospf mpls-te command

Field	Description
Local Interface Address	Local interface address
Remote Interface Address	Remote interface address
TE Metric	TE metric
Maximum bandwidth	Maximum bandwidth
Maximum reservable bandwidth	Maximum reservable bandwidth
Admin Group	Administrative group attribute
Global Pool	Global pool
Unreserved BW [0] to [7]	Available bandwidths at the eight levels in the global pool
Sub Pool	Subpool (only significant for DS-TE LSAs)
Unreserved BW [0] to [7]	Available bandwidths at the eight levels in the subpool
Bandwidth Constraints	Bandwidth constraints (only significant for DS-TE LSAs)
BC 0-1	Two types of bandwidth constraints (only significant for DS-TE LSAs): BC0 and BC1
Local Overbooking Multipliers	Local overbooking multipliers
LOM 0-1	Two local overbooking multipliers (only significant for DS-TE LSAs): LOM 0 and LOM 1

display ospf traffic-adjustment

Syntax **display ospf** [*process-id*] **traffic-adjustment**

View Any view

Parameter *process-id*: OSPF process ID, in the range 1 to 65535.

Description Use the **display ospf traffic-adjustment** command to display the settings of tunnel traffic adjustment (IGP shortcut and forwarding adjacency) for a specified or all OSPF processes.

Example # Display the settings of tunnel traffic adjustment for all OSPF processes.

```
<Sysname> display ospf traffic-adjustment
OSPF Process 100 with Router ID 100.0.0.1
Traffic adjustment
Interface: 100.0.0.1 (Tunnel0)
     Type: Forwarding Adjacency  State: Up
     Neighbor ID: 100.0.0.2   Cost: 100
     Configuration:
     Neighbor Ip Address: 100.0.0.2
     Cost               : -10
     Cost Type          : Relative
     Hold time          : 10s
```

Table 419 Description on the fields of the display ospf traffic-adjustment command

Field	Description
Interface	Tunnel interface address and name

Table 419 Description on the fields of the display ospf traffic-adjustment command

Field	Description
Type	Approach to automatic route advertisement: IGP shortcut or forwarding adjacency
Neighbor ID	Remote neighbor ID
Cost	Cost
State	State: up or down
Neighbor Ip Address	Neighbor IP address
Cost Type	Cost type
Hold time	Hold time

display tunnel-info

Syntax **display tunnel-info** { *tunnel-id* | **all** | **statistics** }

View Any view

Parameter *tunnel-id*: Specifies a tunnel ID, in the range 1 to FFFFFFFE. If a tunnel is specified, only information about this tunnel will be displayed.

all: Display information about all tunnels.

statistics: Displays statistics about tunnels.

Description Use the **display tunnel-info** command to display information about tunnels.

Example # Display information about all tunnels.

```
<Sysname> display tunnel-info all
Tunnel ID           Type              Destination
------------------------------------------------------
0x1100002           lsp               2.2.2.2
```

Display statistics about tunnels.

```
<Sysname> display tunnel-info statistics
Tunnel Allocation Method :    GLOBAL
Avail Tunnel ID Value :       262144

Total Tunnel ID Allocated :   1
LSP :                         1
GRE :                         0
CRLSP :                       0
LOCAL IFNET :                 0
MPLS LOCAL IFNET :            0
```

Table 420 Description on the fields of the display tunnel-info statistics command

Field	Description
Tunnel Allocation Method	The way that tunnels are allocated
Avail Tunnel ID Value	Available tunnel IDs. Available tunnel ID values vary by device.
Total Tunnel ID Allocated	Total number of tunnel IDs that have been allocated

Table 420 Description on the fields of the display tunnel-info statistics command

Field	Description
LSP	Number of LSP tunnels
GRE	Number of GRE tunnels
CRLSP	Number of CR-LSP tunnels
LOCAL IFNET	Number of CE-side interfaces in MPLS L2VPN
MPLS LOCAL IFNET	Number of outgoing interfaces in CCC remote mode in MPLS L2VPN

enable traffic-adjustment

Syntax **enable traffic-adjustment**

undo enable traffic-adjustment

View OSPF view/IS-IS view

Parameter None

Description Use the **enable traffic-adjustment** command to enable IGP shortcut.

Use the **undo enable traffic-adjustment** command to disable IGP shortcut.

By default, IGP shortcut is disabled.

IGP shortcut allows OSPF to include static LSP tunnels in SPF calculation and advertise them to OSPF neighbors.

Example # Enable IGP shortcut when the IGP protocol is OSPF.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable traffic-adjustment
```

Enable IGP shortcut when the IGP protocol is IS-IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] enable traffic-adjustment
```

enable traffic-adjustment advertise

Syntax **enable traffic-adjustment advertise**

undo enable traffic-adjustment advertise

View OSPF view/IS-IS view

Parameter None

Description Use the **enable traffic-adjustment advertise** command to enable forwarding adjacency.

Use the **undo enable traffic-adjustment advertise** command to disable forwarding adjacency.

By default, forwarding adjacency is disabled.

Forwarding adjacency allows OSPF to include static LSP tunnels in SPF calculation but not advertise them to OSPF neighbors.

Example # Enable forwarding adjacency when the IGP protocol is OSPF.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] enable traffic-adjustment advertise
```

Enable forwarding adjacency when the IGP protocol is IS-IS.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] enable traffic-adjustment advertise
```

explicit-path

Syntax **explicit-path** *pathname* [**disable** | **enable**]

undo explicit-path *pathname*

View System view

Parameter *pathname*: Name of an explicit path for a tunnel, a string of 1 to 31 characters.

disable: Disables explicit routing.

enable: Enables explicit routing.

Description Use the **explicit-path** command to create an explicit path and enter its view.

Use the **undo explicit-path** command to remove an explicit path.

Example # Create an explicit path named path1 and enter its view.

```
<Sysname> system-view
[Sysname] explicit-path path1
[Sysname-explicit-path-path1]
```

list hop

Syntax **list hop** [*ip-address*]

View Explicit path view

Parameter *ip-address*: Specifies the IP address of a node on the explicit path. If no IP address is specified, information about all the nodes on the explicit path is displayed.

Description Use the **list hop** command to display information about specified or all nodes on the explicit path.

Example # Display information about all nodes on an MPLS TE explicit path.

```
<Sysname> system-view
[Sysname] explicit-path path1
[Sysname-explicit-path-path1] list hop
Path Name : path1        Path Status :  Enabled
1             1.1.1.9      Strict         Include
2             2.2.2.9      Strict         Exclude
```

modify hop

Syntax **modify hop** *ip-address1 ip-address2* [**include** [**loose** | **strict**] | **exclude**]

View Explicit path view

Parameter *ip-address1 ip-address2*: Substitutes the IP address specified by the *ip-address2* argument for the IP address specified by the *ip-address1* argument in the explicit path. The specified IP addresses could be link IP addresses or router IDs of nodes.

include: Includes the IP address specified by the *ip-address2* argument on the explicit path.

loose: Indicates that the next hop is a loose node which is not necessarily directly connected to the specified node.

strict: Indicates that the next hop is a strict node which must be directly connected to the specified node.

exclude: Excludes the IP address specified by the *ip-address2* argument from subsequent path calculations.

Description Use the **modify hop** command to change the IP address of a node on the explicit path.

By default, the changed IP address is included on the explicit path and its next hop is a strict node.

Example # Replace IP address 10.0.0.125 on explicit path named path1 with IP address 10.0.0.200 and exclude this new IP address from subsequent path calculations.

```
[Sysname-explicit-path-p1] modify hop 10.0.0.125 10.0.0.200 exclude
```

mpls rsvp-te

Syntax **mpls rsvp-te**

undo mpls rsvp-te

View MPLS view, interface view

Parameter None

Description Use the **mpls rsvp-te** command to enable RSVP-TE.

Use the **undo mpls rsvp-te** command to disable RSVP-TE.

By default, RSVP-TE is disabled.

You must enable RSVP-TE before you can configure other RSVP-TE features.

Before enabling RSVP-TE, enable MPLS in both system view and interface view.

Disabling RSVP-TE in MPLS view disables RSVP-TE on interfaces.

Example # Enable RSVP-TE on current node.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te
```

Enable RSVP-TE on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te
```

mpls rsvp-te authentication

Syntax **mpls rsvp-te authentication** { **cipher** | **plain** } *auth-key*

undo mpls rsvp-te authentication

View Interface view

Parameter **cipher**: Indicates that the specified authentication key is a cipher-text key.

plain: Indicates that the specified authentication key is a plain-text key.

auth-key: Authentication key, case sensitive. Input in plain text, the string for it is 8 to 16 characters in length; input in cipher text, the string for it is 24 characters in length. If the **plain** keyword is specified, it can only be input in plain text. If the **cipher** keyword is specified, it can be input in both plain text or in cipher text.

Description Use the **mpls rsvp-te authentication** command to enable RSVP message authentication on the interface.

Use the **undo mpls rsvp-te authentication** command to disable RSVP message authentication on the interface.

The RSVP messages sent out of the interface convey a message authentication digest created using the hash algorithm and the configured authentication key. This authentication key also used by the interface to authenticate received RSVP messages. For the two interfaces at the two ends of a link to exchange RSVP messages, they must share the same authentication key.

This hop-by-hop authentication of RSVP is to prevent fake resource reservation requests from occupying network resources.

Example # Enable RSVP message authentication on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te authentication plain partner123
```

mpls rsvp-te blockade-multiplier

Syntax **mpls rsvp-te blockade-multiplier** *number*

undo mpls rsvp-te blockade-multiplier

View MPLS view

Parameter *number*: Blockade multiplier, in the range 3 to 255.

Description Use the **mpls rsvp-te blockade-multiplier** command to configure the blockade multiplier.

Use the **undo mpls rsvp-te blockade-multiplier** command to restore the default.

The default blockade multiplier is 4.

A ResvErr message establishes blockade state in each node through which it passes to solve the killer reservation problem where one request could deny service to another. The use of blockade state allows a smaller request to be forwarded or established.

The blockade timeout time is determined by the following equation:

Blockade_Expired_Time = Kb × refresh-time

Where, Kb is the blockade multiplier, and refresh-time is the refresh interval for reservation state.

Upon expiration of the blockade timeout time, the blockade state on the node is removed.

Before you can configure this command, enable RSVP-TE.

Related command: **mpls rsvp-te timer refresh**.

Example # Set the blockade multiplier to five.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te blockade-multiplier 5
```

mpls rsvp-te graceful-restart

Syntax **mpls rsvp-te graceful-restart**

undo mpls rsvp-te graceful-restart

View MPLS view

Parameters None

Description Use the **mpls rsvp-te graceful-restart** command to enable the GR capability for MPLS RSVP-TE.

Use the **undo mpls rsvp-te graceful-restart** command to disable MPLS RSVP-TE GR.

By default, GR capability is disabled for MPLS RSVP-TE.

Note that you need to enable RSVP-TE hello extension before enabling RSVP-TE GR.

Examples # Enable MPLS RSVP-TE GR.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.1
[Sysname] mpls
[Sysname-mpls] mpls te
[Sysname-mpls] mpls rsvp-te
[Sysname-mpls] mpls rsvp-te hello
[Sysname-mpls] mpls rsvp-te graceful-restart
```

mpls rsvp-te hello

Syntax **mpls rsvp-te hello**

undo mpls rsvp-te hello

View MPLS view, interface view

Parameter None

Description Use the **mpls rsvp-te hello** command to enable RSVP hello extension.

Use the **undo mpls rsvp-te hello** command to disable RSVP hello extension.

By default, RSVP hello extension is disabled.

RSVP-TE uses the hello mechanism to detect whether an RSVP neighbor is still alive.

Before you can enable RSVP hello extension in interface view, enable RSVP-TE in interface view and RSVP hello extension in MPLS view.

Example # Enable RSVP hello extension in MPLS view.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te hello
```

Enable RSVP hello extension on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te hello
```

mpls rsvp-te hello-lost

Syntax **mpls rsvp-te hello-lost** *times*

undo mpls rsvp-te hello-lost

View MPLS view

Parameter *times*: Maximum number of consecutive hello losses before an RSVP neighbor is considered dead, in the range 3 to 10.

Description Use the **mpls rsvp-te hello-lost** command to configure the maximum number of consecutive hello losses before an RSVP neighbor is considered dead.

Use the **undo mpls rsvp-te hello-lost** command to restore the default.

By default, the RSVP node considers an RSVP neighbor is dead if no response is received after sending three consecutive hellos.

An RSVP node detects whether its RSVP neighbor is still alive by sending hellos regularly. If no response is received after the number of consecutive hellos reaches the specified limit, the RSVP node considers its RSVP neighbor as dead. The failure is handled the same as a link layer communication failure.

Before you can configure this command, enable RSVP-TE.

Related command: **mpls rsvp-te timer hello**.

Example # Set the maximum number of consecutive hello losses before an RSVP neighbor is considered dead to five.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te hello-lost 5
```

mpls rsvp-te keep-multiplier

Syntax **mpls rsvp-te keep-multiplier** *number*

undo mpls rsvp-te keep-multiplier

View MPLS view

Parameter *number*: Keep multiplier, in the range 3 to 255.

Description Use the **mpls rsvp-te keep-multiplier** command to configure the keep multiplier for the path state block (PSB) and reservation state block (RSB).

Use the **undo mpls rsvp-te keep-multiplier** command to restore default.

The default keep multiplier is 3.

The following equation determines the timeout time of the state stored in PSB and RSB:

Expired_Time = (keep-multiplier + 0.5) × 1.5 × refresh-time

Where, refresh-time is the refresh interval for reservation state set by the **mpls rsvp-te timer refresh** command.

Before you can configure the keep multiplier, enable RSVP-TE.

Related command: **mpls rsvp-te timer refresh**.

Example # Set the keep multiplier to five.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te keep-multiplier 5
```

mpls rsvp-te reliability

Syntax **mpls rsvp-te reliability**

undo mpls rsvp-te reliability

View Interface view

Parameter None

Description Use the **mpls rsvp-te reliability** command to enable the reliability mechanism of RSVP-TE, that is, the Message_ID extension mechanism.

Use the **undo mpls rsvp-te reliability** command to disable the reliability mechanism.

Example # Enable the reliability mechanism of RSVP-TE on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te reliability
```

mpls rsvp-te resvconfirm

Syntax **mpls rsvp-te resvconfirm**

undo mpls rsvp-te resvconfirm

View MPLS view

Parameter None

Description Use the **mpls rsvp-te resvconfirm** command to enable reservation confirmation on current node.

Use the **undo mpls rsvp-te resvconfirm** command to disable reservation confirmation.

By default, resource reservation confirmation is disabled.

After the **mpls rsvp-te resvconfirm** command is configured, resource reservation requests will be confirmed.

Example # Enable reservation confirmation on your device.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te resvconfirm
```

mpls rsvp-te srefresh

Syntax **mpls rsvp-te srefresh**

undo mpls rsvp-te srefresh

View Interface view

Parameter None

Description Use the **mpls rsvp-te srefresh** command to enable summary refresh.

Use the **undo mpls rsvp-te srefresh** command to restore the default.

By default, summary refresh is disabled.

Summary refresh (Srefresh) messages refresh path state and reservation state. Enabling summary refresh disables conventional time-driven state refresh.

Example # Enable summary refresh on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te srefresh
```

mpls rsvp-te timer graceful-restart recovery

Syntax **mpls rsvp-te timer graceful-restart recovery** *recovery-time*

undo mpls rsvp-te timer graceful-restart recovery

View MPLS view

Parameters *recovery-time*: RSVP-TE GR recovery interval in seconds, in the range 60 to 300.

Description Use the **mpls rsvp-te timer graceful-restart recovery** command to set the RSVP-TE GR recovery interval.

Use the **undo mpls rsvp-te timer graceful-restart recovery** command to restore the default.

By default, the RSVP-TE GR recovery interval is 300 seconds.

Examples # Set the RSVP-TE GR recovery interval to 100 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te timer graceful-restart recovery 100
```

mpls rsvp-te timer graceful-restart restart

Syntax **mpls rsvp-te timer graceful-restart restart** *restart-time*

undo mpls rsvp-te timer graceful-restart restart

View MPLS view

Parameters *restart-time*: RSVP-TE GR restart interval in seconds, in the range 60 to 300.

Description Use the **mpls rsvp-te timer graceful-restart restart** command to set the RSVP-TE GR restart interval.

Use the **undo mpls rsvp-te timer graceful-restart restart** command to restore the default.

By default, the RSVP-TE GR restart interval is 120 seconds.

Examples # Set the RSVP-TE GR restart interval to 200 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te timer graceful-restart restart 200
```

mpls rsvp-te timer hello

Syntax **mpls rsvp-te timer hello** *timevalue*

undo mpls rsvp-te timer hello

View MPLS view

Parameter *timevalue*: Hello interval, in the range 1 to 60 seconds.

Description Use the **mpls rsvp-te timer hello** command to configure the hello interval.

Use the **undo mpls rsvp-te timer hello** command to restore the default.

The default hello interval is three seconds.

Before configuring this command, enable the hello mechanism in MPLS view.

Related command: **mpls rsvp-te hello**, **mpls rsvp-te hello-lost**.

Example # Set the hello interval to five seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te timer hello 5
```

mpls rsvp-te timer refresh

Syntax **mpls rsvp-te timer refresh** *timevalue*

undo mpls rsvp-te timer refresh

View MPLS view

Parameter *timevalue*: Refresh interval, in the range 10 to 65535 seconds.

Description Use the **mpls rsvp-te timer refresh** command to configure the path/reservation state refresh interval.

Use the **undo mpls rsvp-te timer refresh** command to restore the default.

The default path/reservation state refresh interval is 30 seconds.

Related command: **mpls rsvp-te keep-multiplier**.

Example # Set the path/reservation state refresh interval to 60 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls rsvp-te timer refresh 60
```

mpls rsvp-te timer retransmission

Syntax **mpls rsvp-te timer retransmission** { **increment-value** [*increment-value*] | **retransmit-value** [*retrans-timer-value*] } *

undo mpls rsvp-te timer retransmission

View Interface view

Parameter **increment-value** *increment-value*: Increment value delta, in the range 1 to 10. The default is 1.

retransmit-value *retrans-timer-value*: Initial retransmission interval, in the range 500 to 3000 milliseconds. The default is 500 milliseconds.

Description Use the **mpls rsvp-te timer retransmission** command to enable RSVP message retransmission.

Use the **undo mpls rsvp-te timer retransmission** command to restore the default.

By default, RSVP message retransmission is disabled.

On an interface enabled with the Message_ID (reliability) mechanism, you may configure RSVP message retransmission. After the interface sends an RSVP message, it waits for an acknowledgement. If no ACK is received before the initial retransmission interval (Rf seconds for example) expires, the interface resends the message. After that, the interface resends the message at an exponentially increased retransmission interval equivalent to (1 + Delta) × Rf seconds either until an acknowledgement is received or the retransmission attempt limit RI is reached. The Delta governs the speed with which the interface increases the retransmission interval.

Example # Enable RSVP message retransmission on interface Ethernet 1/0, setting the increment value delta to 2 and the initial retransmission interval to 1000 milliseconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls rsvp-te timer retransmission increment-va
lue 2 retransmit-value 1000
```

mpls te

Syntax **mpls te**

undo mpls te

View MPLS view, interface view

Parameter None

Description Use the **mpls te** command to enable MPLS TE.

Use the **undo mpls te** command to disable MPLS TE.

By default, MPLS TE is disabled.

When performed in MPLS view, the **mpls te** command enables MPLS TE globally and its **undo** form disables MPLS TE and removes all CR-LSPs.

When performed in interface view, the **mpls te** command enables MPLS TE on an interface and its **undo** form disables MPLS TE and removes all CR-LSPs on the interface.

Before you can enable MPLS TE on an interface, enable MPLS TE globally first.

CAUTION: *After changing the MTU of an interface where MPLS TE is enabled, you need to perform the* ***shutdown*** *command and then the* ***undo shutdown*** *command to refresh the TE tunnels on it.*

Example # Enable MPLS TE globally in MPLS view.

```
<Sysname> system-view
[Sysname] mpls lsr-id 1.1.1.9
[Sysname] mpls
[Sysname-mpls] mpls te
```

Enable MPLS TE on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls
[Sysname-Ethernet1/0] mpls te
```

mpls te affinity property

Syntax **mpls te affinity property** *properties* [**mask** *mask-value*]

undo mpls te affinity property

View Tunnel interface view

Parameter *properties*: Link properties affinity attribute of the tunnel, a 32-bit integer in the range 0x0 to 0xFFFFFFFF. Each affinity bit represents a property with a value of 1 or 0.

mask-value: 32-bit mask comprising 0s and 1s, in the range 0x0 to 0xFFFFFFFF. This mask is used when ANDing the link affinity attribute with the link administrative group attribute. The affinity bits corresponding to the 1s in the mask are "do care" bits which must be considered while those corresponding to the 0s in the mask are "don't care" bits.

Description Use the **mpls te affinity property** command to configure the link affinity attribute of the tunnel.

Use the **undo mpls te affinity property** command to restore the default.

The default affinity attribute of the tunnel is 0x00000000 and the mask is 0x00000000.

The affinity attribute of an MPLS TE tunnel identifies the properties of the links that the tunnel can use.

Related command: **mpls te link administrative group**.

Example # Configure the link affinity attribute of tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te affinity property 101 mask 303
```

mpls te auto-bandwidth

Syntax **mpls te auto-bandwidth** { **adjustment** | **collect-bw** } [**frequency** *seconds*] [**max-bw** *max-bandwidth* | **min-bw** *min-bandwidth*] *

undo mpls te auto-bandwidth

View Tunnel interface view

Parameter **adjustment**: Automatically adjusts the bandwidth of the tunnel.

collect-bw: Collects output rates of the tunnel without tuning bandwidth.

seconds: Automatic bandwidth adjustment/information collection interval, in the range 300 to 604800 seconds. This value cannot be less than the sampling interval configured by the **mpls te timer auto-bandwidth** command.

max-bandwidth: Upper limit for bandwidth tuning, in the range 1 to 32000000 kbps.

min-bandwidth: Lower limit for bandwidth tuning, in the range 1 to 32000000 kbps.

Description Use the **mpls te auto-bandwidth adjustment** command to enable automatic bandwidth adjustment for the tunnel.

Use the **mpls te auto-bandwidth collect-bw** command to enable output rate collection.

Use the **undo mpls te auto-bandwidth adjustment** command to disable automatic bandwidth adjustment and output rate collection on the tunnel.

By default, automatic bandwidth adjustment and output rate collection are disabled.

If automatic bandwidth adjustment is enabled, bandwidth tuning happens every 24 hours without upper and lower bandwidth limits.

- *Support for this command varies by default.*
- *Automatic bandwidth adjustment cannot be used together with these commands:* ***mpls te reoptimization****,* ***mpls te route-pinning****,* ***mpls te backup****, and* ***mpls te resv-style ff****.*

Related command: **mpls te timer auto-bandwidth**.

Example # Automatically tune bandwidth for tunnel 0 hourly.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te auto-bandwidth adjustment frequency 3600
```

mpls te backup

Syntax **mpls te backup** { **hot-standby** | **ordinary** }

undo mpls te backup

View Tunnel interface view

Parameter **hot-standby**: Sets the backup mode to hot backup for the tunnel.

ordinary: Sets the backup mode to ordinary backup for the tunnel.

Description Use the **mpls te backup** command to set the backup mode on the tunnel.

Use the **undo mpls te backup** command to restore the default.

By default, tunnel backup is disabled.

- *With backup enabled, the record route flag is automatically set to record reroute regardless of whether the **mpls te record-route** command is configured.*
- *The backup function cannot be used together with these commands: **mpls te reoptimization**, **mpls te auto-bandwidth adjustment**, and **mpls te resv-style ff**.*

Example # Enable hot backup on tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te backup hot-standby
```

mpls te backup bandwidth

Syntax **mpls te backup bandwidth** { *bandwidth* | { **bc0** | **bc1** } { *bandwidth* | **un-limited** } }

undo mpls te backup bandwidth

View Tunnel interface view

Parameter *bandwidth*: Total bandwidth that the bypass tunnel (also called the protection tunnel) can protect, in the range 1 to 32000000 kbps.

bc0: Indicates that only the LSPs using BC0 bandwidth (global bandwidth) can use the bypass tunnel.

bc1: Indicates that only the LSPs using BC1 bandwidth (subpool bandwidth) can use the bypass tunnel.

If neither BC0 nor BC1 is specified, all LSPs can use the bypass tunnel.

un-limited: Puts on limit on total protected bandwidth.

Description Use the **mpls te backup bandwidth** command to configure the total bandwidth and type of LSP that the bypass tunnel can protect.

Use the **undo mpls te backup bandwidth** command to remove the configuration.

By default, bypass tunnels do not protect bandwidth.

If neither BC0 nor BC1 is specified, all LSP can use the bypass tunnel.

This command is not supported when the signaling protocol is CR-LDP.

Example # Tunnel 0 provides protection for LSPs using BC0 bandwidth without protecting bandwidth. Tunnel 1 provides protection for LSPs using BC1 bandwidth and it can protect 1000 kbps bandwidth.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te backup bandwidth bc0 un-limited
[Sysname-Tunnel0] quit
[Sysname] interface tunnel 1
[Sysname-Tunnel1] mpls te backup bandwidth bc1 1000
```

mpls te bandwidth

Syntax **mpls te bandwidth** [**bc0** | **bc1**] *bandwidth*

undo mpls te bandwidth

View Tunnel interface view

Parameter **bc0**: Obtains bandwidth from BC0.

bc1: Obtains bandwidth from BC1.

bandwidth: Bandwidth needed by the MPLS TE tunnel, in the range 1 to 32000000 kbps.

Description Use the **mpls te bandwidth** command to assign bandwidth to the MPLS TE tunnel.

Use the **undo mpls te bandwidth** command to restore the default.

By default, no bandwidth is assigned to MPLS TE tunnels.

If neither the **bc1** keyword nor the **bc0** keyword is specified, bandwidth is assigned using the global bandwidth pool (BC0).

Example # Assign 1000 kbps bandwidth to MPLS TE tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te bandwidth 1000
```

mpls te bandwidth change thresholds

Syntax **mpls te bandwidth change thresholds** { **down** | **up** } *percent*

undo mpls te bandwidth change thresholds { **down** | **up** }

View Interface view

Parameter **down**: Sets the threshold in percentages for IGP to flood when the bandwidth is decreasing. When the percentage of available bandwidth decrease exceeds the threshold, the change is flooded and the traffic engineering database (TEDB) is updated.

up: Sets the IGP flooding threshold in percentages that applies when the bandwidth is increasing. When the percentage of available bandwidth increase exceeds the threshold, the change is flooded and the TEDB is updated.

percent: IGP flooding threshold in percentages, in the range 0 to 100.

Description Use the **mpls te bandwidth change thresholds** command to set the IGP flooding thresholds that apply when bandwidth resources are increasing and decreasing.

Use the **undo mpls te bandwidth change thresholds** command to restore the default.

The default IGP flooding thresholds in both up and down directions are 10.

Example # On interface Ethernet 1/0 configure IGP to flood when the percentage of available bandwidth decrease reaches 100%.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls te bandwidth change thresholds down 100
```

mpls te commit

Syntax **mpls te commit**

View Tunnel interface view

Parameter None

Description Use the **mpls te commit** command to submit current MPLS TE tunnel configuration.

The MPLS TE tunnel configuration you made can take effect only after you perform this command.

Example # Configure an MPLS TE tunnel and submit the configuration.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] tunnel-protocol mpls te
[Sysname-Tunnel0] destination 2.2.2.9
[Sysname-Tunnel0] mpls te commit
```

mpls te cspf

Syntax **mpls te cspf**

undo mpls te cspf

View MPLS view

Parameter None

Description Use the **mpls te cspf** command to enable CSPF on current node.

Use the **undo mpls te cspf** command to disable CSPF on current node.

By default, CSPF is disabled on current node.

Before enabling CSPF, enable MPLS TE in MPLS view.

CSPF provides an approach to path selection in MPLS domains. You must enable CSPF before configuring other CSPF related functions.

Example # Enable CSPF.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te cspf
```

mpls te cspf timer failed-link

Syntax **mpls te cspf timer failed-link** *timer-interval*

undo mpls te cspf timer failed-link

View MPLS view

Parameter *timer-interval*: Failed link timer setting, in the range 0 to 300 seconds. The default is 10 seconds.

Description Use the **mpls te cspf timer failed-link** command to configure the failed link timer.

Use the **undo mpls te cspf timer failed-link** command to restore the default.

Related command: **mpls te cspf**.

Example # Set the failed link timer to 50 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te cspf timer failed-link 50
```

mpls te fast-reroute

Syntax **mpls te fast-reroute**

undo mpls te fast-reroute

View Tunnel interface view

Parameter None

Description Use the **mpls te fast-reroute** command to enable fast reroute (FRR).

Use the **undo mpls te fast-reroute** command to disable FRR.

By default, FRR is disabled.

After FRR is enabled, the record route flag is automatically set to record reroute with label whether the **mpls te record-route label** command is configured or not.

Disable FRR before configuring the **mpls te record-route** command or its **undo** form.

- *This command is not supported when the signaling protocol is CR-LDP.*
- *Fast reroute cannot be used together with the **mpls te resv-style ff** command.*

Example # Reroute MPLS TE tunnel 0 to an available bypass tunnel in case the protected link or node that it traverses fails.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te fast-reroute
```

mpls te fast-reroute bypass-tunnel

Syntax **mpls te fast-reroute bypass-tunnel tunnel** *tunnel-number*

undo mpls te fast-reroute bypass-tunnel tunnel *tunnel-number*

View Interface view

Parameter *tunnel-number*: Bypass tunnel number.

Description Use the **mpls te fast-reroute bypass-tunnel** command to specify a bypass tunnel for the protected interface.

Use the **undo mpls te fast-reroute bypass-tunnel** command to remove the specified bypass tunnel.

You may perform the **mpls te fast-reroute bypass-tunnel** command multiple times to specify multiple bypass tunnels for the protected interface. At present, a maximum of three bypass tunnels can be specified for a protected interface.

When specifying a bypass tunnel, consider the following:

- The state of the tunnel must be up.
- The protected interface is not the outgoing interface in the route entries for the LSP of the bypass tunnel.

- *A bypass tunnel cannot be used for services like VPN at the same time.*
- *This command is not supported when the signaling protocol is CR-LDP.*

Example # Use Tunnel 0 as the bypass tunnel to protect the link connected to interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls te fast-reroute bypass-tunnel tunnel 0
```

mpls te igp advertise

Syntax **mpls te igp advertise** [**hold-time** *value*]

undo mpls te igp advertise

View Tunnel interface view

Parameter **hold-time** *value*: Sets the delay that IGP waits to notify IGP neighbors of the down event of the TE tunnel. It ranges from 0 to 4294967295 milliseconds. The default is 0 milliseconds.

Description Use the **mpls te igp advertise** command to enable IGP to advertise the MPLS TE tunnel as a link to IGP neighbors.

Use the **undo mpls te igp advertise** command to remove the configuration.

By default, IGP does not advertise MPLS TE tunnels to IGP neighbors.

*The **mpls te igp advertise** command cannot be used together with the **mpls te igp shortcut** command.*

Example # Set the hold time to 10000 milliseconds.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te igp advertise hold-time 10000
```

mpls te igp metric

Syntax **mpls te igp metric** { **absolute** *value* | **relative** *value* }

undo mpls te igp metric

View Tunnel interface view

Parameter **absolute** *value*: Assigns an absolute metric to the TE tunnel for path calculation. The *value* argument takes an integer in the range 1 to 65535. This value is directly used for path calculation.

relative *value*: Assigns a relative metric to the TE tunnel for path calculation. The *value* argument takes an integer in the range -10 to +10. The default is 0. The cost of the corresponding IGP path must be added to this relative metric before it can be used for path calculation.

Description Use the **mpls te igp metric** command to assign a metric to the MPLS TE tunnel.

Use the **undo mpls te igp metric** command to restore the default.

By default, TE tunnels take their IGP metrics.

Example # Assign MPLS TE tunnel 0 a relative metric of -1 for enhanced SPF calculation in IGP.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te igp metric relative -1
```

mpls te igp shortcut

Syntax **mpls te igp shortcut** [**isis** | **ospf**]

undo mpls te igp shortcut

View Tunnel interface view

Parameter **isis**: Sets the IGP protocol to IS-IS.

ospf: Sets the IGP protocol to OSPF.

Description Use the **mpls te igp shortcut** command to enable IS-IS or OSPF to consider the MPLS TE tunnel in its enhanced SPF calculation when the tunnel is up. If no IGP protocol is specified, the command applies to both OSPF and IS-IS.

Use the **undo mpls te igp shortcut** command to restore the default.

By default, IGP does not consider MPLS TE tunnels in its enhanced SPF calculation.

*The **mpls te igp shortcut** command cannot be used together with the **mpls te igp advertise** command.*

Example # Enable OSPF and IS-IS to consider TE tunnel 0 in enhanced SPF calculation when the tunnel is up.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te igp shortcut
```

mpls te link administrative group

Syntax **mpls te link administrative group** *value*

undo mpls te link administrative group

View Interface view

Parameter *value*: Link administrative group attribute, in the range 0x00000000 to 0xFFFFFFFF. It is a set of 32 link properties. Each bit represents a property with a value of 0 or 1. By ANDing the administrative group attribute bits with the corresponding link affinity attribute bits of an MPLS TE tunnel, MPLS TE identifies the properties of the links that the MPLS TE tunnel can use.

Description Use the **mpls te link administrative group** command to configure the link administrative group attribute.

Use the **undo mpls te link administrative group** command to restore the default.

The default link administrative group attribute is 0x00000000.

The interface properties are propagated globally and are used for path selection at the tunnel ingress.

Related command: **mpls te affinity property**.

Example # Assign interface Ethernet 1/0 the link administrative group attribute of 0x00000101.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls te link administrative group 101
```

mpls te loop-detection

Syntax **mpls te loop-detection**

undo mpls te loop-detection

View Tunnel interface view

Parameter None

Description Use the **mpls te loop-detection** command to configure the node to perform loop detection when setting up the MPLS TE tunnel.

Use the **undo mpls te loop-detection** command to disable loop detection.

Loop detection is disabled by default.

Example # Configure the node to perform loop detection when setting up tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te loop-detection
```

mpls te max-link-bandwidth

Syntax **mpls te max-link-bandwidth** *bandwidth-value* [**bc1** *bc1-bandwidth*]

undo mpls te max-link-bandwidth

View Interface view

Parameter *bandwidth-value*: Maximum link bandwidth available for RSVP traffic, in the range 1 to 32000000 kbps.

bc1 *bc1-bandwidth*: Reservable bandwidth in kbps on the interface, in the range 1 to *bandwidth-value*.

Description Use the **mpls te max-link-bandwidth bandwidth-value** command to configure maximum link bandwidth.

Use the **undo mpls te max-link-bandwidth** command to remove the configuration.

The configured maximum bandwidth is available for both MPLS traffic and common best-effort traffic.

Example # On interface Serial 1/0 set maximum link bandwidth available for RSVP traffic to 1158 kbps, and the reservable bandwidth to 200 kbps.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] mpls te max-link-bandwidth 1158 bc1 200
```

mpls te max-reservable-bandwidth

Syntax **mpls te max-reservable-bandwidth** *bandwidth-value* [**bc1** *bc1-bandwidth*]

undo mpls te max-reservable-bandwidth

View Interface view

Parameter *bandwidth-value*: Maximum reservable bandwidth for RSVP traffic, in the range 1 to 32000000 kbps (global pool bandwidth).

bc1 *value*: Reservable bandwidth in kbps on the interface, in the range 1 to *bandwidth-value* (subpool bandwidth).

Description Use the **mpls te max-reservable-bandwidth** command to configure the maximum reservable bandwidth.

Use the **undo mpls te max-reservable-bandwidth** command to remove the configuration.

The bandwidth in this command is configured only for MPLS traffic.

Example # On interface Ethernet 1/0 set maximum reservable bandwidth for MPLS TE to 1158 kbps, and the reservable BC1 bandwidth to 200 kbps.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls te max-reservable-bandwidth 1158 bc1 200
```

mpls te metric

Syntax **mpls te metric** *value*

undo mpls te metric

View Interface view

Parameter *value*: TE metric of the link, in the range 0 to 4294967295.

Description Use the **mpls te metric** command to assign a TE metric to the link.

Use the **undo mpls te metric** command to restore the default.

By default, the link uses its IGP metric as its TE metric.

Related command: **mpls te path metric-type**.

Example # Assign a TE metric of 20 to the link on interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls te metric 20
```

mpls te path explicit-path

Syntax **mpls te path explicit-path** *pathname*

undo mpls te path

View Tunnel interface view

Parameter *pathname*: Name of an MPLS-TE explicit path, a string of 1 to 31 characters.

Description Use the **mpls te path explicit-path** command to associate an explicit path with the tunnel.

Use the **undo mpls te path** command to remove the association.

Example # Configure interface Tunnel0 to use the explicit path named path1.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te path explicit-path path1
```

mpls te path metric-type

Syntax **mpls te path metric-type** { **igp** | **te** }

undo mpls te path metric-type

View MPLS view, tunnel interface view

Parameter **igp**: Uses IGP metric for tunnel routing.

te: Uses TE metric for tunnel routing.

Description Use the **mpls te path metric-type** command in MPLS view to specify the link metric type used for routing tunnels not configured with link metric type.

Use the **mpls te path metric-type** command in tunnel interface view to specify the link metric type used for routing current tunnel.

Use the **undo mpls te path metric-type** command to restore the default. This **undo** form is only available in tunnel interface view.

By default, TE metrics of links are used in path calculation for TE tunnels.

Related command: **mpls te metric**.

Example In MPLS view:

Use the IGP metrics of links in path calculation for TE tunnels not configured with link metric type.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te path metric-type igp
```

In tunnel interface view:

Use the IGP metrics of links for routing tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te path metric-type igp
```

mpls te priority

Syntax **mpls te priority** *setup-priority* [*hold-priority*]

undo mpls te priority

View Tunnel interface view

Parameter *setup-priority*: Setup priority of the tunnel, in the range 0 to 7. A lower numerical number indicates a higher priority.

hold-priority: Holding priority of the tunnel, in the range 0 to 7. A lower numerical number indicates a higher priority. If not configured, it is the same as the setup priority.

Description Use the **mpls te priority** command to assign a setup priority and holding priority to the MPLS TE tunnel.

Use the **undo mpls te priority** command to restore the default.

By default, both setup and holding priorities of TE tunnels are 7.

To avoid flapping caused by improper preemptions between TE tunnels, the setup priority of an MPLS TE tunnel should not be set higher than its holding priority.

Example # Set the setup and holding priorities of TE tunnel 0 to 1.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te priority 1
```

mpls te record-route

Syntax **mpls te record-route** [**label**]

undo mpls te record-route

View Tunnel interface view

Parameter **label**: Includes the record of labels in the route record. This keyword is not supported when the signaling protocol is CR-LDP. This keyword is not supported when the signaling protocol is CR-LDP.

Description Use the **mpls te record-route** command to enable route recording or label recording.

Use the **undo mpls te record-route** command to restore the default.

By default, route recording and label recording are disabled.

Example # Enable route recording on MPLS TE tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te record-route
```

mpls te reoptimization (user view)

Syntax **mpls te reoptimization**

View User view

Parameter None

Description Use the **mpls te reoptimization** command to start reoptimizing all reoptimization-enabled TE tunnels.

Example # Start reoptimizing all reoptimization-enabled TE tunnels.

```
<Sysname> mpls te reoptimization
```

mpls te reoptimization (tunnel interface view)

Syntax **mpls te reoptimization** [**frequency** *seconds*]

undo mpls te reoptimization

View Tunnel interface view

Parameter *seconds*: Reoptimization frequency, in the range 1 to 604800 seconds. The default is 3600 seconds, or 1 hour.

Description Use the **mpls te reoptimization** command to enable reoptimization on the tunnel.

Use the **undo mpls te reoptimization** command to disable reoptimization on the tunnel.

Reoptimization is disabled by default.

The reoptimization function cannot be used together with these commands:

mpls te auto-bandwidth adjustment, **mpls te route-pinning**, **mpls te backup**, and **mpls te resv-style ff**.

Example # Enable reoptimization, setting the reoptimization (automatic rerouting) frequency to 43200 seconds (12 hours).

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te reoptimization frequency 43200
```

mpls te resv-style

Syntax **mpls te resv-style** { **ff** | **se** }

undo mpls te resv-style

View Tunnel interface view

Parameter **ff**: Sets the resource reservation style to fixed filter (FF).

se: Sets the resource reservation style to shared explicit (SE).

Description Use the **mpls te resv-style** command to set the resource reservation style for the MPLS TE tunnel.

Use the **undo mpls te resv-style** command to restore the default.

The default resource reservation style is SE.

You may configure FF and SE only when the signaling protocol is set to RSVP-TE.

Example # Adopt the FF reservation style when setting up the CR-LSP tunnel for TE tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te resv-style ff
```

mpls te retry

Syntax **mpls te retry** *times*

undo mpls te retry

View Tunnel interface view

Parameter *times*: Number of tunnel setup retries, in the range 1 to 4294967295.

Description Use the **mpls te retry** command to configure the maximum number of tunnel setup retries.

Use the **undo mpls te retry** command to restore the default.

The default maximum number of tunnel setup retries is 5.

You may configure the system to attempt setting up a tunnel multiple times until it is established successfully or until the number of attempts reaches the upper limit.

Related command: **mpls te timer retry**.

Example # Set the maximum number of tunnel setup retries to 10.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te retry 10
```

mpls te route-pinning

Syntax **mpls te route-pinning**

undo mpls te route-pinning

View Tunnel interface view

Parameter None

Description Use the **mpls te route-pinning** command to enable route pinning.

Use the **undo mpls te route-pinning** command to restore the default.

By default, route pinning is disabled.

*The **mpls te route-pinning** command cannot be used together with the **mpls te reoptimization** command and the **mpls te auto-bandwidth adjustment** command.*

Example # Enable route pinning.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te route-pinning
```

mpls te signal-protocol

Syntax **mpls te signal-protocol { crldp | rsvp-te | static }**

View Tunnel interface view

Parameter **rsvp-te**: Sets the signaling protocol for MPLS TE tunnel establishment to RSVP-TE.

crldp: Sets the signaling protocol for MPLS TE tunnel establishment to CR-LDP.

static: Sets up the tunnel using a static CR-LSP.

Description Use the **mpls te signal-protocol** command to configure the signaling protocol for MPLS TE tunnel establishment.

The default signaling protocol for MPLS TE tunnel establishment is RSVP-TE.

CAUTION: *To use RSVP-TE as the signaling protocol for setting up the MPLS TE tunnel, you must enable both MPLS TE and RSVP-TE on the interface for the tunnel to use.*

Example # Adopt CR-LDP as the signaling protocol for establishing MPLS TE tunnel 0.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te signal-protocol crldp
```

mpls te tie-breaking

Syntax **mpls te tie-breaking { least-fill | most-fill | random }**

undo mpls te tie-breaking

View MPLS view, tunnel interface view

Parameter **least-fill**: Selects a path with the least bandwidth usage ratio (the used bandwidth to the maximum reservable link bandwidth).

most-fill: Selects a path with the most bandwidth usage ratio (the used bandwidth to the maximum reserved bandwidth).

random: Selects a path randomly.

Description Use the **mpls te tie-breaking** command to specify a tie breaker for CSPF to route a tunnel when multiple paths are present with the same metric.

Use the **undo mpls te tie-breaking** command to restore the default.

By default, the **random** keyword applies.

The tie breaker configured in MPLS TE tunnel interface view has higher priority over the one configured in MPLS view.

Example # Configure CSPF to route tunnels over paths with the least bandwidth usage ratio.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te tie-breaking least-fill
```

Configure CSPF to route tunnel 0 over a path with the least bandwidth usage ratio in MPLS TE interface view.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te tie-breaking least-fill
```

mpls te timer auto-bandwidth

Syntax **mpls te timer auto-bandwidth** [*seconds*]

undo mpls te timer auto-bandwidth

View MPLS view

Parameter *seconds*: Interval for output rate sampling for tunnels configured with automatic bandwidth adjustment, in the range 1 to 604800 seconds. If it is not configured, the default of 300 seconds applies. You are recommended to use the default in normal cases.

Description Use the **mpls te timer auto-bandwidth** command to enable automatic bandwidth adjustment and set the interval for output rate sampling for tunnels governed by automatic bandwidth adjustment.

Use the **undo mpls te timer auto-bandwidth** command to restore the default.

By default, automatic bandwidth adjustment is disabled.

- *Support for this command varies by default.*
- *To change the output rate sampling interval, use the **undo mpls te timer auto-bandwidth** command to disable automatic bandwidth adjustment first and then use the **mpls te timer auto-bandwidth** command to re-configure it.*

Related command: **mpls te auto-bandwidth**.

Example # Collect the output rates of MPLS TE tunnels automatically every 10 seconds or 600 seconds.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te timer auto-bandwidth 600
```

mpls te timer fast-reroute

Syntax **mpls te timer fast-reroute** [*seconds*]

undo mpls te timer fast-reroute

View MPLS view

Parameter *seconds*: FRR polling timer setting for the point of local repair (PLR) to poll available bypass tunnels for the best one. It ranges from 0 to 604800 seconds, with 0 disabling the PLR to poll available bypass tunnels regularly for the best one. The default is 300 seconds or 5 minutes.

Description Use the **mpls te timer fast-reroute** command to set the FRR polling timer.

Use the **undo mpls te timer fast-reroute** command to disable FRP polling.

The default FRR polling timer is 300 seconds.

This command is not supported when the signaling protocol is CR-LDP.

Example # Set the FRR polling timer to 120 seconds or 2 minutes.

```
<Sysname> system-view
[Sysname] mpls
[Sysname-mpls] mpls te timer fast-reroute 120
```

mpls te timer retry

Syntax **mpls te timer retry** *second*

undo mpls te timer retry

View Tunnel interface view

Parameter *second*: Interval for re-establishing the tunnel, in the range 1 to 4294967295 seconds.

Description Use the **mpls te timer retry** command to configure the interval for re-establishing the tunnel.

Use the **undo mpls te timer retry** command to restore the default.

The default interval for re-establishing a tunnel is 10 seconds.

Related command: **mpls te retry**.

Example # Set the interval for re-establishing tunnel 0 to 20 seconds.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te timer retry 20
```

mpls te tunnel-id

Syntax **mpls te tunnel-id** *tunnel-id*

View Tunnel interface view

Parameters *tunnel-id*: Tunnel ID. The value range and default vary by device.

Description Use the **mpls te tunnel-id** command to configure the tunnel ID.

You need to configure the tunnel ID before issuing the **mpls te commit** command for the first time. Otherwise, the tunnel cannot be created.

Once configured, a tunnel ID cannot be removed. To change a tunnel ID, you need to remove the tunnel and then reconfigure the tunnel, giving it a new tunnel ID.

Examples # Configure the tunnel ID as 100.

```
<Sysname> system-view
[Sysname] interface tunnel 1/0/0
[Sysname-Tunnel1/0/0] mpls te tunnel-id 100
```

mpls te vpn-binding

Syntax **mpls te vpn-binding** { **acl** *acl-number* | **vpn-instance** *vpn-instance-name* }

undo mpls te vpn-binding

View Tunnel interface view

Parameter *acl-number*: Referenced ACL number, in the range 3000 to 3999. The MPLS TE tunnel forwards only VPN instance traffic that matches the referenced ACL.

vpn-instance-name: VPN instance name, a string of 1 to 31 characters. The MPLS TE tunnel forwards only traffic of the specified VPN instance.

Description Use the **mpls te vpn-binding** command to define the traffic that can travel the MPLS TE tunnel.

Use the **undo mpls te vpn-binding** command to restore the default.

By default, no restriction is defined about what traffic can travel down a TE tunnel.

Example # Configure tunnel 0 to forward only traffic of VPN 1.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te vpn-binding vpn-instance vpn1
```

Configure tunnel 0 to forward only traffic that matches ACL 3001.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule 0 permit ip vpn-instance vpn1
[Sysname-acl-adv-3001] quit
[Sysname] interface tunnel 0
[Sysname-Tunnel0] mpls te vpn-binding acl 3001
[Sysname-Tunnel0] mpls te commit
```

mpls-te enable

Syntax **mpls-te enable**

undo mpls-te

View OSPF area view

Parameter **enable**: Enables the MPLS TE capability in the OSPF area.

Description Use the **mpls-te enable** command to enable the MPLS TE capability in current OSPF area.

Use the **undo mpls-te** command to disable the MPLS TE capability in current OSPF area.

By default, the MPLS TE capability is disabled in OSPF areas.

For an OSPF area to support the MPLS TE capability, its OSPF process must be available with the opaque LSA capability.

Related command: **opaque-capability**.

Example # Enable the MPLS TE capability in OSPF area 1.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] area 1
[Sysname-ospf-100-area-0.0.0.1] mpls-te enable
```

next hop

Syntax **next hop** *ip-address* [**include** [**loose** | **strict**] | **exclude**]

View Explicit path view

Parameter *ip-address*: Defines a node by its link IP address or router ID in dotted decimal notation. In the strict routing approach, this IP address must be a link IP address. In the loose routing approach, this IP address can be either a link IP address or router ID.

include: Includes the specified IP address on the explicit path.

loose: Indicates that the next hop is a loose node which is not necessarily directly connected to current node.

strict: Indicates that the next hop is a strict node which must be directly connected to current node.

exclude: Excludes the specified IP address from the explicit path.

Description Use the **next hop** command to define a node on the explicit path. By performing this command multiple times, you may define all nodes that the explicit path must traverse in sequence.

By default, next hops are strict hops on an explicit path.

Related command: **delete hop**.

Example # Exclude IP address 10.0.0.125 from the MPLS TE explicit path p1.

```
[Sysname-explicit-path-p1] next hop 10.0.0.125 exclude
```

opaque-capability

Syntax **opaque-capability enable**

undo opaque-capability

View OSPF view

Parameter **enable**: Enables the opaque LSA capability.

Description Use the **opaque-capability** command to enable the opaque LSA capability for the OSPF process to generate and receive from its neighbors Opaque LSAs.

Use the **undo opaque-capability** command to restore the default.

By default, the opaque LSA capability of OSPF is disabled.

Example # Enable the opaque LSA capability of OSPF.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] opaque-capability enable
```

reset mpls rsvp-te statistics

Syntax **reset mpls rsvp-te statistics** { **global** | **interface** [*interface-type interface-number*]

View User view

Parameter **global**: Clears statistics about global RSVP-TE.

interface: Clears statistics about RSVP-TE for all interfaces.

interface *interface-type interface-number*: Specifies an interface by its type and number. If an interface is specified, the command clears the statistics about RSVP-TE for the interface.

Description Use the **reset mpls rsvp-te statistics** command to clear statistics about RSVP-TE.

Example # Clear statistics about global RSVP-TE.

```
<Sysname> reset mpls rsvp-te statistics global
```

reset mpls te auto-bandwidth adjustment timers

Syntax **reset mpls te auto-bandwidth adjustment timers**

View User view

Parameter None

Description Use the **reset mpls te auto-bandwidth adjustment timers** command to reset the automatic bandwidth adjustment function.

This command clears information about output rate sampling and the remaining time for next bandwidth optimization.

Support for this command varies by default.

Example # Reset the automatic bandwidth adjustment function.

```
<Sysname> reset mpls te auto-bandwidth adjustment timers
```

static-cr-lsp egress

Syntax **static-cr-lsp egress** *tunnel-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label-value* [**lsrid** *ingress-lsr-id* **tunnel-id** *tunnel-id*]

undo static-cr-lsp egress *tunnel-name*

View System view

Parameter *Tunnel-name*: Tunnel name comprising 1 to 15 characters.

interface-type interface-number: Specifies an interface by its type and number.

in-label-value: Incoming label, in the range 16 to 1023.

ingress-lsr-id: Ingress LSR ID, in the format of an IP address.

tunnel-id: Tunnel ID, in the range 1 to 65534.

Description Use the **static-cr-lsp egress** command to configure a static CR-LSP on the egress node.

Use the **undo static-cr-lsp egress** command to remove the static CR-LSP.

Example # Configure a static CR-LSP on the egress node, setting its name to tunnel24, incoming interface to Serial 1/0, and incoming label to 233.

```
<Sysname> system-view
[Sysname] static-cr-lsp egress tunnel34 incoming-interface serial 1/
0 in-label 233
```

static-cr-lsp ingress

Syntax **static-cr-lsp ingress** *tunnel-name* **destination** *dest-addr* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label-value* [**bandwidth** [**bc0** | **bc1**] *bandwidth-value*]

undo static-cr-lsp ingress *tunnel-name*

View System view

Parameter *tunnel-name*: Name of the tunnel, a case sensitive string of 1 to 15 characters. It must be an exact reference to a tunnel created by the **interface tunnel** command.

next-hop-addr: Next hop address.

outgoing-interface *interface-type interface-number*: Specifies an outgoing interface for the static CR-LSP.

out-label-value: Outgoing label, in the range 16 to 1023.

bc0: Obtains bandwidth from a subpool.

bc1: Obtains bandwidth from the global pool.

bandwidth-value: Bandwidth assigned to the CR-LSP, in the range 1 to 32000000 kbps.

Description Use the **static-cr-lsp ingress** command to configure a static CR-LSP at the ingress node.

Use the **undo static-cr-lsp ingress** command to remove the static CR-LSP.

The next hop address cannot be a local public address when configuring the static CR-LSP on the ingress or a transit node.

Example # Configure a static CR-LSP on the ingress node, setting its name to Tunnel3, destination IP address to 202.25.38.1, destination address mask length to 24, next hop IP address to 202.55.25.33, outgoing label to 237, and required bandwidth to 20 kbps.

```
<Sysname> system-view
[Sysname] static-cr-lsp ingress Tunnel3 destination 202.25.38.1 next
hop 202.55.25.33 out-label 237 bandwidth 20
```

static-cr-lsp transit

Syntax **static-cr-lsp transit** *tunnel-name* **incoming-interface** *interface-type interface-number* **in-label** *in-label-value* { **nexthop** *next-hop-addr* | **outgoing-interface** *interface-type interface-number* } **out-label** *out-label-value* [**bandwidth** [**bc0** | **bc1**] *bandwidth-value*]

undo static-cr-lsp transit *tunnel-name*

View System view

Parameter *Tunnel-name*: Tunnel name comprising 1 to 15 characters.

next-hop-addr: Next hop address.

outgoing-interface *interface-type interface-number*: Specifies an outgoing interface for the static CR-LSP.

in-label-value: Incoming label, in the range 16 to 1023.

out-label-value: Outgoing label, in the range 16 to 1023.

bc0: Obtains bandwidth from a subpool.

bc1: Obtains bandwidth from the global pool.

bandwidth-value: Bandwidth assigned to the CR-LSP, in the range 1 to 32000000 kbps.

Description Use the **static-cr-lsp transit** command to configure a static CR-LSP on a transit node.

Use the **undo static-cr-lsp transit** command to remove the static CR-LSP.

The next hop address cannot be a local public address when configuring the static CR-LSP on the ingress or a transit node.

Example # Configure a static CR-LSP on the transit node, setting its name to tunnel34, incoming interface to Serial 1/0, incoming label to 123, outgoing interface to Serial 1/1, outgoing label to 253, and required bandwidth to 20 kbps.

```
<Sysname> system-view
[Sysname] static-cr-lsp transit tunnel34 incoming-interface serial 1/0 in-la
bel 123 outgoing-interface serial 1/1 out-label 253 bandwidth 20
```

te-set-subtlv

Syntax **te-set-subtlv** { **bw-constraint** *value* | **lo-multiplier** *value* | **unreserved-bw-sub-pool** *value* } *

undo te-set-subtlv { **bw-constraint** | **lo-multiplier** | **unreserved-bw-sub-pool** } *

View IS-IS view

Parameter **bw-constraint**: Sets the bandwidth constraint sub-TLV.

lo-multiplier: Sets the sub-TLV of local overbooking multiplier (LOM).

unreserved-bw-sub-pool: Sets the sub-TLV of unreserved subpool bandwidth.

value: Sub-TLV in the range 19 to 254.

Description Use the **te-set-subtlv** command to configure the sub-TLVs carrying the DS-TE parameters. As no standard is available for these sub-TLVs, you need to configure them manually for interoperability with other vendors' devices.

Use the **undo te-set-subtlv** command to restore the default.

By default, the bandwidth constraint sub-TLV is 252, the sub-TLV of LOM is 253, and the sub-TLV of unreserved subpool bandwidth is 251.

Related command: **display isis traffic-eng sub-tlvs**.

Example # Configure sub-TLVs for IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] te-set-subtlv bw-constraint 200 lo-multiplier 201 u
nreserve-bw-sub-pool 202
```

traffic-eng

Syntax **traffic-eng** [**level-1** | **level-1-2** | **level-2**]

undo traffic-eng [**level-1** | **level-1-2** | **level-2**]

View IS-IS view

Parameter **level-1**: Enables Level-1 IS-IS TE.

level-1-2: Enables Level-1-2 IS-IS TE.

level-2: Enables Level-2 IS-IS TE.

If no level is specified, IS-IS TE applies to Level-1-2.

Description Use the **traffic-eng** command to enable IS-IS TE.

Use the **undo traffic-eng** command to restore the default.

By default, IS-IS TE is disabled.

*In order to enable IS-IS TE, you must use the **cost-style** command to configure the cost style of the IS-IS packet to wide, compatible or wide-compatible. Refer to "cost-style" on page 1040.*

Example # Enable TE for Level-2 IS-IS process 1.

```
<Sysname> system-view
[Sysname] isis 1
[Sysname-isis-1] cost-style compatible
[Sysname-isis-1] traffic-eng level-2
```

97 MPLS L2VPN CONFIGURATION COMMANDS

ccc interface in-label out-label

Syntax

ccc *ccc-connection-name* **interface** *interface-type interface-number* **in-label** *in-label-value* **out-label** *out-label-value* { **nexthop** *ip-address* | **out-interface** *interface-type interface-number* } [**control-word** | **no-control-word**]

undo ccc *ccc-connection-name*

View System view

Parameter

ccc-connection-name: Name for the CCC connection, a string of 1 to 20 characters. It is used for uniquely identifying a CCC connection on a PE.

interface-type interface-number: Specifies the interface connecting the local CE by its type and number.

in-label-value: Incoming label, in the range 16 to 1023.

out-label-value: Outgoing label, in the range 16 to 1023.

nexthop *ip-address*: Specifies the IP address of the next hop.

out-interface *interface-type interface-number*: Specifies the outgoing interface by its type and number.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description

Use the **ccc interface in-label out-label** command to create a remote CCC connection between CEs connected to different PEs.

Use the **undo ccc** command to delete a CCC connection.

This command must be configured on both of the PEs.

A PE uses connection names to identify different CCC connections. A CCC connection can have different names on different PEs.

If a P router is connected with a PE, you must configure a static LSPs between them.

Currently, only L2VPNs using ATM, PPP, FR, or HDLC encapsulation support the control word option.

*If the outgoing interface is an Ethernet or VLAN interface, you need to use the **nexthop** ip-address combination to specify the IP address of the next hop. Otherwise, you need to use the **out-interface** interface-type interface-number combination to specify the outgoing interface.*

Example # Create a remote CCC connection from CEA to CEB, setting the incoming interface to that connecting CEA, namely Serial 2/0; the outgoing interface to that connecting the P router, namely Serial 2/1; the incoming label to 100; and the outgoing label to 200.

```
<Sysname> system-view
[Sysname] ccc CEA-CEB interface serial 2/0 in-label 100 out-label 20
0 out-interface serial 2/1
```

ccc interface out-interface

Syntax **ccc** *ccc-connection-name* **interface** *interface-type interface-number* **out-interface** *interface-type interface-number*

undo ccc *ccc-connection-name*

View System view

Parameter *ccc-connection-name*: Name for the CCC connection, a string of 1 to 20 characters. It is used for uniquely identifying a CCC connection on a PE.

interface *interface-type interface-number*: Specifies the interface for connecting the first CE by its type and number.

out-interface *interface-type interface-number*: Specifies the interface for connecting the second CE by its type and number.

Description Use the **ccc interface out-interface** command to create a local CCC connection between two CEs connected to the same PE.

Use the **undo ccc** command to delete a CCC connection.

Example # Create a local CCC connection between two CEs connected to the same PE.

```
<Sysname> system-view
[Sysname] ccc ccc-connect-1 interface ethernet 1/0 out-interface ethernet 1/1
```

ce

Syntax **ce** *ce-name* [**id** *ce-id* [**range** *ce-range*] [**default-offset** *ce-offset*]]

undo ce *ce-name*

View MPLS L2VPN view/MPLS L2VPN CE view

Parameter *ce-name*: Unique name for a CE in the current VPN of the current PE, a string of 1 to 20 characters that cannot include the character of "-".

ce-id: ID for the CE in the VPN. For MSR20 series routers, it is in the range of 0 to 199; for MSR30 and MSR50 series routers, it is in the range 0 to 249.

ce-range: Maximum number of CEs that the current PE can support. For MSR20 series routers, it is in the range of 1 to 200; for MSR30 and MSR50 series routers, it is in the range 1 to 250. The default is 10.

ce-offset: Original CE offset. It can be either 0 or 1. The default is 0.

Description Use the **ce** command in MPLS L2VPN view to create a CE and enter MPLS L2VPN CE view.

Use the **ce** command in MPLS L2VPN CE view to create another CE.

Use the **undo ce** command to delete a CE.

Example # Create a CE named ce1 for a VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 100:1
[Sysname-mpls-l2vpn-vpn1] ce ce1 id 1
[Sysname-mpls-l2vpn-ce-vpn1-ce1]
```

Create a CE named ce2 for a VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 100:1
[Sysname-mpls-l2vpn-vpn1] ce ce1 id 1
[Sysname-mpls-l2vpn-ce-vpn1-ce1] ce ce1 id 2
[Sysname-mpls-l2vpn-ce-vpn1-ce2]
```

connection

Syntax **connection** [**ce-offset** *id*] **interface** *interface-type interface-number* [**tunnel-policy** *tunnel-policy-name*]

undo connection { **ce-offset** *id* | **interface** *interface-type interface-number* }

View MPLS L2VPN CE view

Parameter *id*: ID of the peer CE of the L2VPN connection. For MSR20 series routers, it is in the range of 0 to 199; for MSR30 and MSR50 series routers, it is in the range 0 to 249.

interface-type interface-number: Specifies the interface connecting the CE by its type and number. The encapsulation type must be same as that of the VPN.

tunnel-policy-name: Tunneling policy for the VC, a string of 1 to 19 characters.

Description Use the **connection** command to create a Kompella connection.

Use the **undo connection** command to delete a Kompella connection on a CE interface.

When creating a Kompella connection, you must specify the ID of the peer CE and the local CE interface.

If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number of one.

Related command: **tunnel select-seq load-balance-number** on page 1718.

Example # Create a Kompella connection.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1
[Sysname-mpls-l2vpn-vpn1] ce ce1
[Sysname-mpls-l2vpn-ce-vpn1-ce1] connection ce-offset 1 interface serial 2/0
```

display bgp l2vpn

Syntax **display bgp l2vpn** { **all** | **group** [*group-name*] | **peer** [[*ip-address*] **verbose**] | **route-distinguisher** *route-distinguisher* [**ce-id** *ce-id* [**label-offset** *label-offset*]] }

View Any view

Parameter **all**: Displays all L2VPN information.

group-name: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

verbose: Displays detailed information.

route-distinguisher: Route distinguisher in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters.

ce-id: VPN CE ID of the MPLS L2VPN connection, in the range 0 to 65535. A remote connection requires the remote CE number.

label-offset: Label offset, in the range 0 to 65,535.

Description Use the **display bgp l2vpn** command to display information about BGP L2VPN in the BGP routing table.

Related command: **route-distinguisher (MPLS L2VPN view)**.

Example # Display all information about L2VPN in the BGP routing table.

```
<Sysname> display bgp l2vpn all

BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 bgp.l2vpn: 1 destination
 Route Distinguisher: 100:1
 CE ID   Label Offset   Label Base    nexthop          pref   as-path

 1       0              8202          3.3.3.9          100
```

Table 421 Description on the fields of the display bgp l2vpn all command

Field	Description
BGP Local router ID	BGP local router ID
Local AS number	Local AS number
Origin codes	Route origin codes, which can be: i - IGP: Indicates that the network layer reachability information is from within the AS e - EGP: Indicates that the network layer reachability information is learned through EGP ? - incomplete: Indicates that the network layer reachability information is learned through other ways
bgp l2vpn	Number of BGP L2VPNs
Route Distinguisher	RD
CE ID	CE number in the VPN
Label Offset	Label offset
Label Base	Label base
nexthop	IP address of the next hop
pref	Local preference
as-path	AS-PATH of the route

Display brief information about L2VPN peers in the BGP routing table.

```
<Sysname> display bgp l2vpn peer
 BGP local router ID : 4.4.4.9
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 0

  Peer        V    AS   MsgRcvd   MsgSent  OutQ PrefRcv Up/Down  State    PrefRcv

  3.3.3.9     4   100      20      22     0     00:15:30 Established  0
```

Table 422 Description on the fields of the display bgp l2vpn peer command

Field	Description
BGP local router ID	ID of the local BGP router
Local AS number	Local AS number
Total number of peers	Number of peers
Peers in established state	Number of peers with BGP sessions in the state of established
Peer	IP address of the peer
V	BGP version that the peer is using
AS	AS number
MsgRcvd	Number of messages received

Table 422 Description on the fields of the display bgp l2vpn peer command

Field	Description
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration that the BGP session is in the current status
State	Status of the peer

Display detailed information about L2VPN peer 3.3.3.9 in the BGP routing table.

```
<Sysname> display bgp l2vpn peer 3.3.3.9 verbose
          Peer: 3.3.3.9   Local: 2.2.2.9
          Type: IBGP link
          BGP version 4, remote router ID 3.3.3.9
          BGP current state: Established, Up for   00:21:15
          BGP current event: KATimerExpired
          BGP last state: OpenConfirm
          Port:  Local - 179      Remote - 1034
          Configured: Active Hold Time: 180 sec   Keep Alive Time:60 sec
          Received  : Active Hold Time: 180 sec
          Negotiated: Active Hold Time: 180 sec
          Peer optional capabilities:
          Peer support bgp multi-protocol extended
          Peer support bgp route refresh capability
          Address family IPv4 Unicast: advertised and received
          Address family L2VPN: advertised and received
 Received: Total 26 messages, Update messages 2
 Sent: Total 28 messages, Update messages 2
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 15 seconds
 Peer Preferred Value: 0
 Routing policy configured:
 No routing policy is configured
```

Table 423 Description on the fields of the display bgp l2vpn peer verbose command

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP current state	Current status of the BGP session
BGP current event	Current event of the BGP session
BGP last state	Last status of the BGP session
Port	Ports used by the BGP session, one is local or the other remote
Configured	Settings of the local timers
Received	Settings of the remote timers
Negotiated	Negotiated settings of the timers
Peer optional capabilities:	Optional peer capabilities, including the support for BGP multicast protocol extension and the support for BGP route refreshing
Peer support bgp multi-protocol extended	
Peer support bgp route refresh capability	
Address family IPv4 Unicast	IPv4 unicast address family capability

Table 423 Description on the fields of the display bgp l2vpn peer verbose command

Field	Description
Address family L2VPN	L2VPN address family
Received	Total number of received messages and that of received update messages
Sent	Total number of sent messages and that of received update messages
Maximum allowed prefix number	Maximum number of routes allowed
Threshold	Threshold value
Routing policy configured	Routing policy specified for the peer

Display L2VPN information with the RD being 100:1 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 bgp.l2vpn: 1 destination
 CE ID   Label Offset   Label Base    nexthop         pref    as-path
 4       0              132096        3.3.3.9         100
```

Table 424 Description on the fields of display bgp l2vpn route-distinguisher

Field	Description
BGP Local router ID	BGP local router ID
local AS number	Local AS number
Origin codes	Route origin codes, which can be: i - IGP: Indicates that the network layer reachability information is from within the AS e - EGP: Indicates that the network layer reachability information is learned through EGP ? - incomplete: Indicates that the network layer reachability information is learned through other ways
bgp l2vpn	Number of BGP L2VPNs
Route Distinguisher	RD
CE ID	CE number in the VPN
Label Offset	Label offset
Label Base	Label base
nexthop	IP address of the next hop
pref	Preference
as-path	AS-PATH of the route

Display L2VPN information with the RD being 100:1 and the CE ID being 4 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1 ce-id 4
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 CE ID   Label Offset   Label Base    nexthop          pref   as-path
 1       0              8202          3.3.3.9          100
```

Table 425 Description on the fields of display bgp l2vpn route-distinguisher ce-id

Field	Description
BGP Local router ID	BGP local router ID
local AS number	Local AS number
Origin codes	Route origin codes, which can be: i - IGP: Indicates that the network layer reachability information is from within the AS e - EGP: Indicates that the network layer reachability information is learned through EGP ? - incomplete: Indicates that the network layer reachability information is learned through other ways
Route Distinguisher	RD
CE ID	CE number in the VPN
Label Offset	Label offset
Label Base	Label base
nexthop	IP address of the next hop
pref	Preference
as-path	AS-PATH of the route

Display L2VPN information with the RD being 100:1, the CE ID being 4, and the label offset being 0 in the BGP routing table.

```
<Sysname> display bgp l2vpn route-distinguisher 100:1 ce-id 4 label-offset 0
BGP Local router ID : 2.2.2.9, local AS number : 100
 Origin codes:i - IGP, e - EGP, ? - incomplete
 nexthop:3.3.3.9,  pref :100,     as-path :
 label base:132096,label range:10,layer-2 mtu:0,encap type:Unknown or Reserv
ed
  label            state
  132096           down
  132097           up
  132098           down
  132099           down
  132100           down
  132101           down
  132102           down
  132103           down
  132104           down
  132105           down
```

Table 426 Fields of display bgp l2vpn route-distinguisher ce-id label-offset

Field	Description
BGP Local router ID	BGP local router ID
local AS number	Local AS number
Origin codes	Route origin codes, which can be: i - IGP: Indicates that the network layer reachability information is from within the AS e - EGP: Indicates that the network layer reachability information is learned through EGP ? - incomplete: Indicates that the network layer reachability information is learned through other ways
nexthop	IP address of the next hop
pref	Preference

Table 426 Fields of display bgp l2vpn route-distinguisher ce-id label-offset

Field	Description
as-path	AS-PATH of the route
label base	Label base
label range	Label range
layer-2 mtu	Layer 2 MTU
encap type	Encapsulation type

display ccc

Syntax **display ccc** [**ccc-name** *ccc-name* | **type** { **local** | **remote** }]

View Any view

Parameter *ccc-name*: CCC connection name, a string of 1 to 20 characters.

type: Specifies the type of the CCC connections.

local: Specifies local CCC connections.

remote: Specifies remote CCC connections.

Description Use the **display ccc** command to display information about CCC connections.

If you do not specify the connection name or type, this command displays information about all CCC connections.

Example # Display information about CCC connection c1.

```
<Sysname> display ccc ccc-name c1
***Name                    : c1
   Type                    : remote
   State                   : down
   Intf                    : Serial2/0 (up)
   In-label                : 100
   Out-label               : 200
   Nexthop                 : 20.1.1.1
```

Display information about all local CCC connections.

```
<Sysname> display ccc type local
***Name                    : c2
   Type                    : local
   State                   : up
   Intf1                   : Serial2/0 (up)
   Intf2                   : Serial2/1 (up)
```

Display information about all CCC connections.

```
<Sysname> display ccc
    Total  ccc vc          : 1
    Local  ccc vc          : 0,  0 up
```

```
    Remote ccc vc           : 1,  0 up
***Name                     : c1
    Type                    : remote
    State                   : down
    Intf                    : Serial2/0 (up)
    In-label                : 100
    Out-label               : 200
    Nexthop                 : 20.1.1.1
```

Table 427 Description on the fields of the display ccc command

Field	Description
Total ccc vc	Total number of CCC connections
Local ccc vc	Number of local CCC connections
Remote ccc vc	Number of remote CCC connections
Name	Name of the CCC connection
Type	Type of the CCC connection
State	Status of the CCC connection
Intf	Interface of the CCC connection
In-label	Incoming label
Out-label	Outgoing label
Nexthop	IP address of the next hop

display l2vpn ccc-interface vc-type

Syntax **display l2vpn ccc-interface vc-type** { **all** | **bgp-vc** | **ccc** | **ldp-vc** | **static-vc** } [**up** | **down**]

View Any view

Parameter **all**: Specifies interfaces of any encapsulation types.

bgp-vc: Specifies interfaces of Kompella L2VPN VCs.

ccc: Specifies interfaces of CCC L2VPN VCs.

ldp-vc: Specifies interfaces of Martini L2VPN VCs.

static-vc: Specifies interfaces of SVC L2VPN VCs.

up: Specifies CCC interfaces in the state of UP.

down: Specifies CCC interfaces in the state of DOWN.

Description Use the **display l2vpn ccc-interface vc-type** command to display information about specified L2VPN VC interfaces.

Example # Display information about interfaces of any encapsulation types.

```
<Sysname> display l2vpn ccc-interface vc-type all
Total ccc-interface of CCC VC: 3
```

```
up (3), down (0)
Interface     Encap Type  State   VC Type
Serial2/0     ppp         up      CCC
Serial2/1     ppp         up      bgp-vc
Serial2/2     ppp         up      static-vc
```

Display information about interfaces of Kompella L2VPN VCs.

```
<Sysname> display l2vpn ccc-interface vc-type bgp-vc
Total ccc-interface of BGP VC: 1
up (1), down (0)
Interface     Encap Type  State   VC Type
Serial2/1     ppp         up      bgp-vc
```

Display information about interfaces of SVC L2VPN VCs that are in the state of UP.

```
<Sysname> display l2vpn ccc-interface vc-type svc-vc up
Total ccc-interface of SVC VC: 1,
up (1), down (0)
Interface     Encap Type  State   VC Type
Serial2/2     ppp         up      static-vc
```

Table 428 Description on the fields of display l2vpn ccc-interface vc-type

Field	Description
Total ccc-interface of XXX VC	Total interface number of L2VPN VCs of type xxx
Interface	Name of the interface
Encap Type	Encapsulation type of the interface
State	Status of the interface
VC Type	Encapsulation type of the L2VPN VC interface

display mpls l2vc

Syntax **display mpls l2vc** [**interface** *interface-type interface-number* | **remote-info**]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies the interface connecting the CE by its type and number.

remote-info: Specifies Martini VCs from the remote peer.

Description Use the **display mpls l2vc** command to display information about Martini VCs configured on the router.

If you specify an interface, the command displays information about Martini VCs configured on the CE interface.

Example # Display information about all Martini VCs configured on the router.

```
<Sysname> display mpls l2vc
total  ldp vc : 3     0 up       3 down
```

```
Transport   Client       VC      Local      Remote     Tunnel
VC ID       Intf         State   VC Label   VC Label   Policy
5           Serial2/0    down    0          0          lsp3
6           Serial2/1    down    0          0          lsp2
7           Serial2/2    down    0          0          plcy3
```

Table 429 Description on the fields of the display mpls l2vc command

Field	Description
total ldp vc	Total number of Martini VCs
Transport VC ID	Remote VC ID
Client Intf	Interface connected with the CE
VC State	Status of the VC
Local VC Label	Local VC label
Remote VC Label	Remote VC label
Tunnel Policy	Tunnel policy configured

Display information about all Martini VCs configured on interface Ethernet 1/0.

```
<Sysname> display mpls l2vc interface ethernet 1/0
***VC ID                 : 10000000
    VC State             : up
    Destination          : 1.1.1.1
    Client Intf          : Ethernet1/0 is up
    Local Group ID       : 0
    Remote Group ID      : 0
    Local VC Label       : 1029
    Remote VC Label      : 1029
    Tunnel Policy        : default
    Tunnel Type          : lsp
    Tunnel ID            : 0x220020
```

Table 430 Description on the fields of the display mpls l2vc interface command

Field	Description
VC ID	Remote VC ID
VC State	Status of the VC
Destination	Destination IP address
Client Intf	Interface connected with the CE
Local Group ID	Local VC group ID, used for the L2VPN VC FEC TLV field of LDP messages
Remote Group ID	Remote VC group ID, used for the L2VPN VC FEC TLV field of LDP messages
Local VC Label	Local VC label
Remote VC Label	Remote VC label
Tunnel Policy	Tunnel policy configured
Tunnel Type	Type of the tunnel
Tunnel ID	ID of the tunnel

Display information about Martini VCs received from the remote peer.

```
<Sysname> display mpls l2vc remote-info
total remote ldp vc : 1
Transport  Group      Peer            Remote     Remote     C     Remote
```

```
VC ID       ID          Addr            Encap       VC Label    Bit    MTU
100         0           3.3.3.9         ppp         1025        0      1500
```

Table 431 Description on the fields of the display mpls l2vc remote-info command

Field	Description
total remote ldp vc	Total number of remote LDP VCs
Transport VC ID	Remote VC ID
Group ID	Remote VC group ID, used for the L2VPN VC FEC TLV field of LDP messages
Peer Addr	IP address of the peer
Remote Encap	Encapsulation type of the remote interface
Remote VC Label	Remote VC label
C Bit	Control word, which can be 0 or 1
Remote MTU	MTU of the remote interface

display mpls l2vpn

Syntax **display mpls l2vpn** [**export-route-target-list** | **import-route-target-list** | **vpn-name** *vpn-name* [**local-ce** | **remote-ce**]]

View Any view

Parameter **export-route-target-list**: Displays the export route target list.

import-route-target-list: Displays the import route target list.

vpn-name: VPN name, a case insensitive string of 1 to 31 characters that cannot include the character of "-".

local-ce: Displays the configurations and status of all local CEs of a specified VPN.

remote-ce: Displays the configurations and status of remote CEs learned from other PEs.

Description Use the **display mpls l2vpn** command to display information about L2VPNs configured on a PE.

If you do not specify a VPN, the command displays information about all L2VPNs.

Example # Display the L2VPN export route target list.

```
<Sysname> display mpls l2vpn export-route-target-list
export vpn target list: 755:7  888:8
```

Table 432 Description on the fields of display mpls l2vpn export-route-target-list

Field	Description
export vpn target list	BGP VPN export route target list

Display information about all L2VPNs configured on the PE.

```
<Sysname> display mpls l2vpn
VPN Number: 1
 vpn-name  encap-type  route-distinguisher     mtu   ce(L)  ce(R)
vpn2      atm aal5    500:1                  888   0      0
```

Table 433 Description on the fields of the display mpls l2vpn command

Field	Description
VPN Number	Number of created VPNs
vpn-name	Name of the VPN
encap-type	Encapsulation type
route-distinguisher	RD
mtu	Maximum transmission unit
ce(L)	Local CE number
ce(R)	Remote CE number

Display information about L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1
***VPN name               : vpn1
    Encap type             : vlan
    Local ce number(s)     : 0
    Remote ce number(s)    : 0
    Route distinguisher    : 100:2
    MTU                    : 1500
    Import vpn target      : 111:1
    Export vpn target      : 111:1
```

Table 434 Description on the fields of the display mpls l2vpn vpn-name command

Field	Description
VPN Name	Name of the VPN
Encap type	Encapsulation type
Local ce number(s)	Local CE number
Remote ce number(s)	Remote CE number
Route-distinguisher	RD
Mtu	Maximum transmission unit
Import vpn target	Incoming VPN target
Export vpn target	Outgoing VPN target

Display information about local CEs of L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1 local-ce
ce-name              ce-id   range   conn-num  LB
ce1                  1       10      0         132096/0/10
LB stands for label block
```

Table 435 Description on the fields of display mpls l2vpn vpn-name local-ce

Field	Description
ce-name	Name of the CE
ce-id	CE number
range	CE range
conn-num	Number of connections

Table 435 Description on the fields of display mpls l2vpn vpn-name local-ce

Field	Description
LB	Label block

Display information about remote CEs of L2VPN vpn1.

```
<Sysname> display mpls l2vpn vpn-name vpn1 remote-ce
no.  ce-id peer-id         route-distinguisher     LB
1    4     3.3.3.9         100:1                   132096/0/10
```

Table 436 Description on the fields of display mpls l2vpn vpn-name remote-ce

Field	Description
no	Sequence number
ce-id	CE ID
peer-id	IP address of the peer
route-distinguisher	RD
LB	Label block

display mpls l2vpn connection

Syntax **display mpls l2vpn connection** [**vpn-name** *vpn-name* [**remote-ce** *ce-id* | **down** | **up** | **verbose**]]

display mpls l2vpn connection [**interface** *interface-type interface-number* | **summary**]

View Any view

Parameter *vpn-name*: VPN name, a case insensitive string of 1 to 31 characters that cannot include the character of "-".

ce-id: ID of the remote CE for the L2VPN connection, in the range 0 to 249.

down: Displays detailed information about the connections that are down.

up: Displays detailed information about the connections that are up. If you specify neither the **down** nor the **up** keyword, the command displays detailed information about connections that are either up or down.

verbose: Displays detailed information. This keyword is valid only when displaying information about all connections in a VPN.

interface *interface-type interface-number*: Specifies an interface by its type and number.

summary: Displays summary information about connections.

Description Use the **display mpls l2vpn connection** command to display information about Kompella L2VPN connections.

If you do not specify any argument, the command displays information about all Kompella L2VPN connections.

Example # Display information about all Kompella L2VPN connections.

```
<Sysname> display mpls l2vpn connection
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
VPN name: vpn1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
  CE name: ce1, id: 1,
  Rid type status peer-id         route-distinguisher   intf
  4   rmt  up     3.3.3.9         100:1                 Serial2/0
```

Table 437 Description on the fields of the display mpls l2vpn connection command

Field	Description
connections	Statistics about connections, including the number of connections in the state of Up, the number of connections in the state of Down, the number of local connections, the number of remote connections, and the number of unknown connections
VPN name	Name of the VPN
CE name	Name of the CE
id	ID of the CE
Rid	ID of the remote CE
type	Type of the connection
status	Status of the connection
peer-id	IP address of the peer
route-distinguisher	RD
intf	Interface for the connection

Display information about Kompella L2VPN connections for VPN vpn1.

```
<Sysname> display mpls l2vpn connection vpn-name vpn1
VPN name: vpn1,
1 total connections,
connections: 1 up, 0 down, 0 local, 1 remote, 0 unknown
  CE name: ce1, id: 1,
  Rid type status peer-id         route-distinguisher   intf
  4   rmt  up     3.3.3.9         100:1                 Serial2/0
```

For descriptions of the output fields of the command, see Table 437.

Display information about Kompella L2VPN connections on interface Serial 2/0.

```
<Sysname> display mpls l2vpn connection interface Serial 2/0
***Conn-type              : remote
   Local vc state         : up
   Remote vc state        : up
   Local ce-id            : 1
   Local ce name          : ce1
   Remote ce-id           : 4
   Intf(state,encap)      : Serial2/0 (up,ppp)
   Peer id                : 3.3.3.9
   Route-distinguisher    : 100:1
```

```
  Local vc label          : 132100
  Remote vc label         : 132097
  Tunnel policy           : policy1
  Tunnel Type             : lsp
  Tunnel ID               : 0x226013
```

Table 438 Description on the fields of display mpls l2vpn connection interface

Field	Description
Conn-type	Type of the connection
Local vc state	Local VC status
Remote vc state	Remote VC status
Local ce-id	ID of the local CE
Local ce name	Name of the local CE
Remote ce-id	ID of the remote CE
Intf(state,encap)	Interface name (interface status, interface encapsulation type)
Peer id	IP address of the peer
Route-distinguisher	RD
Local vc label	Local VC label
Remote vc label	Remote VC label
Tunnel policy	Name of the tunneling policy
Tunnel type	Type of the tunnel
Tunnel ID	ID of the tunnel

Display summary information about all Kompella L2VPN connections.

```
<Sysname> display mpls l2vpn connection summary
1 total connections,
connections: 1 up,  0 down , 0 local, 1 remote, 0 unknown
No.   vpn-name    local-num remote-num unknown-num up-num total-num
1     vpn1        0         1          0           1      1
```

Table 439 Description on the fields of mpls l2vpn connection summary

Field	Description
connections	Statistics about connections, including the number of connections in the state of Up, the number of connections in the state of Down, the number of local connections, the number of remote connections, and the number of unknown connections
No.	Sequence number
vpn-name	Name of the VPN
local-num	Number of local connections
remote-num	Number of remote connections
unknown-num	Number of unknown connections
up-num	Number of connections that are up
total-num	Total number of connections

display mpls l2vpn forwarding-info

Syntax **display mpls l2vpn forwarding-info** [*vc-label*] **interface** *interface-type interface-number* [| { **begin** | **exclude** | **include** } *regular-expression*]

View Any view

Parameter *vc-label*: L2VPN VC label, in the range 16 to 4294967295.

interface-type interface-number: Specifies an interface by its type and number.

|: Filters the output information.

begin: Displays information starting with the specified string.

include: Displays information including the specified string.

exclude: Displays information excluding the specified string.

regular-expression: Regular expression, a string of 1 to 80 characters that cannot contain any blank space.

Description Use the **display mpls l2vpn forwarding-info** command to display MPLS L2VPN forwarding information.

Example # Display MPLS L2VPN forwarding information.

```
<Sysname> display mpls l2vpn forwarding-info interface Serial 2/0
VCLABEL TUNNELTYPE ENTRYTYPE OUTINTERFACE
----------------------------------------
1025    LSP        SEND      Serial2/0
   1   Record(s) Found.
```

Table 440 Description on the fields of display mpls l2vpn forwarding-info

Field	Description
VCLABEL	VC label
TUNNELTYPE	Tunnel type
ENTRYTYPE	Forwarding entry type
OUTINTERFACE	Outgoing interface
Record(s) Found	Number of discovered records

display mpls static-l2vc

Syntax **display mpls static-l2vc** [**interface** *interface-type interface-number*]

View Any view

Parameter **interface** *interface-type interface-number*: Specifies a CE interface by its type and number.

Description Use the **display mpls static-l2vc** command to display information about static VCs configured on the router.

If you specify an interface, the command displays only information about static VCs configured on the CE interface.

Example # Display information about all static VCs configured on the router.

```
<Sysname> display mpls static-l2vc
total connections:  1,  1 up,  0 down
ce-intf         state destination     tr-label  rcv-label tnl-policy
Serial2/0       up    3.3.3.9         100       200       policy1
```

Table 441 Description on the fields of the display mpls static-l2vc command

Field	Description
total connections	Statistics about connection, including the total number of connections, number of connections that are up, and number of connections that are down
ce-intfe	CE interface
State	Status of the VC
destination	Destination IP address
tr-label	Outgoing label
rcv-label	Incoming label
tnl-policy	Name of the tunneling policy

Display information about static VCs configured on interface Serial 2/0.

```
<Sysname> display mpls static-l2vc interface Serial 2/0
***CE-interface           : Serial2/0 is up
   VC State               : up
   Destination            : 3.3.3.9
   Transmit-vpn-label     : 100
   Receive-vpn-label      : 400
   Tunnel Policy          : policy1
   Tunnel Type            : lsp
   Tunnel ID              : 0x226013
```

Table 442 Description on the fields of display mpls static-l2vc interface

Field	Description
CE-interface	Name of the CE interface
VC State	Status of the VC
Destination	Destination IP address
Transmit-vpn-label	Outgoing label
Receive-vpn-label	Incoming label
Tunnel Policy	Name of the tunneling policy
Tunnel Type	Type of the tunnel
Tunnel ID	ID of the tunnel

l2vpn-family

Syntax **l2vpn-family**

undo l2vpn-family

View BGP view

Parameter None

Description Use the **l2vpn-family** command to enter BGP L2VPN address family view.

Use the **undo l2vpn-family** command to delete all configurations for the BGP L2VPN address family.

Example # Enter BGP L2VPN address family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn]
```

mpls l2vc

Syntax **mpls l2vc** *destination vcid* [**tunnel-policy** *tunnel-policy-name*] [**control-word** | **no-control-word**]

undo mpls l2vc

View Interface view

Parameter *destination*: IP address of the peer PE.

vc-id: VC ID of the L2VPN connection, in the range 1 to 4294967295.

tunnel-policy-name: Tunneling policy for the VC, a string of 1 to 19 characters.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description Use the **mpls l2vc** command to create a Martini L2VPN connection.

Use the **undo mpls l2vc** command to delete the Martini connection on the CE interface.

- If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number of one.
- Currently, only L2VPNs using ATM, PPP, FR, or HDLC encapsulation support the control word option.

Related command: **tunnel select-seq load-balance-number** on page 1718.

Example # Create a Martini MPLS L2VPN connection.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] mpls l2vc 2.2.2.9 999
```

mpls l2vpn

Syntax **mpls l2vpn**

undo mpls l2vpn

View System view

Parameter None

Description Use the **mpls l2vpn** command to enable MPLS L2VPN.

Use the **undo mpls l2vpn** command to disable MPLS L2VPN and delete all L2VPN configurations.

You must use the **mpls l2vpn** command to enable MPLS L2VPN before configuring the other L2VPN commands.

Example # Enable MPLS L2VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn
```

mpls l2vpn vpn-name

Syntax **mpls l2vpn** *vpn-name* [**encapsulation** { **atm-aal5** | **ethernet** | **fr** | **hdlc** | **ppp** | **vlan** } [**control-word** | **no-control-word**]]

undo mpls l2vpn *vpn-name*

View System view/MPLS L2VPN view

Parameter *vpn-name*: Name for the VPN, a case insensitive string of 1 to 31 characters that cannot include the character of "-". It is used to identify a VPN uniquely on a PE.

encapsulation: Specifies the VPN encapsulation type.

atm-aal5: Uses ATM AAL5 encapsulation.

ethernet: Uses Ethernet encapsulation.

fr: Uses FR encapsulation.

hdlc: Uses HDLC encapsulation.

ppp: Uses PPP encapsulation.

vlan: Uses VLAN encapsulation.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description Use the **mpls l2vpn** command to create a Kompella VPN and enter MPLS L2VPN view.

Use the **undo mpls l2vpn** command to delete a VPN.

The encapsulation type specified here must match that of the CE interface.

Currently, only L2VPNs using ATM, PPP, FR, or HDLC encapsulation support the control word option.

Example # Create Kompella VPN named vpn1 and enter MPLS L2VPN view.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ppp
[Sysname-mpls-l2vpn-vpn1]
```

Create Kompella VPN named vpn2 and enter MPLS L2VPN view.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ppp
[Sysname-mpls-l2vpn-vpn1] mpls l2vpn vpn2 encapsulation ethernet
[Sysname-mpls-l2vpn-vpn2]
```

mpls static-l2vc destination

Syntax **mpls static-l2vc destination** *destination-router-id* **transmit-vpn-label** *transmit-label-value* **receive-vpn-label** *receive-label-value* [**tunnel-policy** *tunnel-policy-name*] [**control-word** | **no-control-word**]

undo mpls static-l2vc

View Interface view

Parameter *dest-router-id*: Destination router ID.

transmit-label-value: Outgoing label for the VPN, namely the outgoing label for the static level 2 VC. The value ranges from 16 to 1023.

receive-label-value: Incoming label for the VPN, namely the incoming label for the static level 2 VC. The value ranges from 16 to 1023.

tunnel-policy-name: Tunneling policy for the VC, a string of 1 to 19 characters.

control-word: Enables the control word option.

no-control-word: Disables the control word option.

Description Use the **mpls static-l2vc destination** command to create a static VC between CEs connected to different PEs.

Use the **undo mpls static-l2vc** command to delete the static VC.

- You must configure the command on both PEs. The destination address is the IP address of the peer PE. The outgoing label and incoming label are respectively the incoming label and outgoing label of the peer.
- If you do not specify the tunneling policy, or specify the tunneling policy name but do not configure the policy, the default policy is used. The default tunneling policy uses LSP tunnels and the load balance number is one.
- Currently, only L2VPNs using ATM, PPP, FR, or HDLC encapsulation support the control word option.

Example # Create a static VC between CEs connected to different PEs.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mpls static-l2vc destination 1.1.1.1 transmit-
vpn-label 111 receive-vpn-label 222 tunnel-policy pol1
```

mtu (MPLS L2VPN view)

Syntax **mtu** *mtu*

undo mtu

View MPLS L2VPN view

Parameter *mtu-value*: MTU for the L2VPN. It ranges from 128 to 1,500 and defaults to 1,500.

Description Use the **mtu** command to set the maximum transmission unit (MTU) for the kompella connections.

Use the **undo mtu** command to restore the default.

*The **mtu** command is not recommended because it affects only negotiation of protocol parameters that may take place and does not affect the forwarding.*

Example # Set the MTU for Kompella connections to 1000.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1
[Sysname-mpls-l2vpn-vpn1] mtu 1000
```

reset bgp l2vpn

Syntax **reset bgp l2vpn** { *as-number* | *ip-address* | **all** | **external** | **internal** }

View User view

Parameter *as-number*: Resets L2VPN BGP connections with the peers in the AS with this number. The AS number must be in the range 1 to 65535.

ip-address: Resets the L2VPN BGP connection to the peer with this IP address.

all: Resets all L2VPN BGP connections.

external: Resets L2VPN EBGP sessions.

internal: Resets L2VPN IBGP sessions.

Description Use the **reset bgp l2vpn** command to reset L2VPN BGP connections.

Example # Reset all L2VPN BGP connections.

```
<Sysname> reset bgp l2vpn all
```

route-distinguisher (MPLS L2VPN view)

Syntax **route-distinguisher** *route-distinguisher*

View MPLS L2VPN view

Parameter *route-distinguisher*: Specifies the route distinguisher (RD) in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters.

An RD can be in either of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

Description Use the **route-distinguisher** command to configure an RD for the VPN.

Different VPNs on a PE must have different RDs, while a VPN can have the same or different RDs on different PEs.

- *You cannot change an RD directly; you can only delete the VPN and then re-create the VPN using the new RD.*
- *No RD is configured by default; you must configure an RD for each VPN. A VPN takes effect only when it is configured with an RD.*
- *Once you configure an RD for a VPN, you cannot remove the association between the RD and the VPN.*

Example # Configure the RD of a VPN.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ppp
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 300:1
```

vpn-target (MPLS L2VPN view)

Syntax **vpn-target** *vpn-target*&<1-16> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | { *vpn-target*&<1-16> [**both** | **export-extcommunity** | **import-extcommunity**] } }

View MPLS L2VPN view

Parameter *vpn-target*: VPN target extended community attributes to be added to the import or export VPN target extended community list, in the format of nn:nn or IP-address:nn. It can be a string of 3 to 21 characters. &<1-16> means that you can specify this argument for up to 16 times.

A VPN target can be in either of the following formats:

- 16-bit AS number:32-bit user-defined number. For example, 101:3.
- 32-bit IP address:16-bit user-defined number. For example, 192.168.122.15:1.

both: Specifies both the export and import VPN extended communities. This is the default.

export-extcommunity: Specifies the export VPN extended community.

import-extcommunity: Specifies the import VPN extended community.

all: Specifies both the import and export VPN extended communities.

Description Use the **vpn-target** command to associate a particular VPN with one or more VPN targets.

Use the **undo vpn-target** command to delete the VPN target(s) associated with a particular VPN.

There is no default value for a VPN target. You must configure it when creating the VPN.

Example # Associate VPN vpn1 with VPN targets.

```
<Sysname> system-view
[Sysname] mpls l2vpn vpn1 encapsulation ppp
[Sysname-mpls-l2vpn-vpn1] route-distinguisher 300:1
[Sysname-mpls-l2vpn-vpn1] vpn-target 1:1 2:2 export-extcommunity
[Sysname-mpls-l2vpn-vpn1] vpn-target 1.2.3.4:11 import-extcommunity
```

98 MPLS L3VPN CONFIGURATION COMMANDS

For information about BGP L2VPN address family, refer to "MPLS L2VPN Configuration Commands" on page 1645.

apply access-vpn vpn-instance

Syntax **apply access-vpn vpn-instance** *vpn-instance-name*&<1-6>

undo apply access-vpn vpn-instance [*vpn-instance-name*]&<1-6>

View Policy routing view

Parameter *vpn-instance-name*&<1-6>: VPN instance name, a string of 1 to 31 characters. &<1-6> means that you can enter one to six VPN instance names.

Description Use the **apply access-vpn vpn-instance** command to specify one or more VPN instances for forwarding packets on a policy node.

Use the **undo apply access-vpn vpn-instance** command to remove one or more VPN instances from the policy node.

You can set up to six VPN instances for one node in a policy. Packets matching the criteria are forwarded by the first valid VPN instance routing table.

With no VPN instance name specified, the **undo apply access-vpn vpn-instance** command removes all VPN instances from the FIB.

Note that the VPN instances you specify for the **apply access-vpn vpn-instance** command must exist.

For configuration about policy routing, refer to "IP Unicast Policy Routing Configuration Commands" on page 807.

Example # Specify to use VPN instances vpn1 and vpn2 for forwarding.

```
<Sysname> system-view
[Sysname] policy-based-route policy1 permit node 10
[Sysname-policy-based-route] apply access-vpn vpn-instance vpn1 vpn2
```

default local-preference (BGP-VPNv4 subaddress family view)

Syntax **default local-preference** *value*

undo default local-preference

View BGP-VPNv4 subaddress family view

Parameter *value*: Default value for the local preference, in the range 0 to 4294967295. A greater value represents a higher priority.

Description Use the **default local-preference** command to set the default value of the local preference.

Use the **undo default local-preference** command to restore the default.

By default, the default value of the local preference is 100.

Example # With devices A and B connected to the outside AS, configure B with a default local preference of 180 in BGP-VPNv4 subaddress family view, allowing the route going through B to be preferred when more than one route is present.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] default local-preference 180
```

default med (BGP-VPNv4 subaddress family view)

Syntax **default med** *med-value*

undo default med

View BGP-VPNv4 subaddress family view

Parameter *med-value*: MED value, in the range 0 to 4,294,967,295.

Description Use the **default med** command to set the default system metric.

Use the **undo default med** command to restore the default.

With other criteria the same, the system selects the route with a smaller MED value as the AS external route.

By default, the MED value is 0.

Example # Set the default MED to 10 for PE 1 in BGP-VPNv4 subaddress family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] default med 10
```

description (VPN instance view)

Syntax **description** *text*

undo description

View VPN instance view

Parameter *text*: Description for the VPN instance, a string of 1 to 80 characters.

Description Use the **description** command to configure a description for a VPN instance.

Use the **undo description** command to delete the description.

Example # Configure the description of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] description This is vpn1
```

display bgp vpnv4 all routing-table

Syntax **display bgp vpnv4 all routing-table** [*network-address* [{ *mask* | *mask-length* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13> [**no-export-subconfed** | **no-advertise** | **no-export**] * [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **different-origin-as** | **peer** *ip-address* { **advertised-routes** | **received-routes** } [**statistic**] | **regular-expression** *as-regular-expression* | **statistic**]

View Any view

Parameter *network-address*: IP address of the destination segment.

mask-length: Length of the network mask, in the range 0 to 32.

mask-address: Network mask, in the format of X.X.X.X.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays classless inter-domain routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list in the routing table.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

different-origin-as: Displays information about routes with different AS origins.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Specifies the routing information sent to the specified peer.

received-routes: Specifies the routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS_PATH regular expression.

statistic: Displays BGP VPNv4 route statistics.

Description Use the **display bgp vpnv4 all routing-table** command to display all BGP VPNv4 routing information.

Example # Display all BGP VPNv4 routing information.

```
<Sysname> display bgp vpnv4 all routing-table

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Total number of routes from all PE: 2
 Route Distinguisher: 100:1

    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1         (1025 /NULL )    0          100
```

```
*>i 123.1.1.1/32       1.1.1.1         (1024 /NULL )    0          100

 Total routes of vpn-instance vpn1: 5
    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1                          0          100
*>  10.1.1.0/24        0.0.0.0         (NULL /1025 )    0
*>  20.0.0.0           10.1.1.1        (NULL /1026 )    0
*>i 123.1.1.1/32       1.1.1.1                          0          100
*>  124.1.1.1/32       0.0.0.0         (NULL /1024 )    0
```

Table 443 Description on the fields of display bgp vpnv4 all routing-table

Field	Description
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. Valid values include: * - valid: Valid route > - best: Best route d - damped: Route damped for route flap h - history: History route i - internal: Internal route s - suppressed: Suppressed route S - Stale: Stale route
Origin	Route origin codes. Valid values include: i - IGP (learned from the AS) e - EGP (learned through EGP) ? - incomplete (learned in any other way)
Total number of routes from all PE	Total number of VPNv4 routes from all PEs
Route Distinguisher	RD
Network	Network address
NextHop	Address of the next hop
Label(recv/app)	Incoming and outgoing labels
MED	Metric associated with the destination network
Total routes of vpn-instance vpn1	Total number of routes of the specified VPN instance
LocPrf	Local preference

display bgp vpnv4 group

Syntax **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **group** [*group-name*]

View Any view

Parameter **all**: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of the BGP peer group, a string of 1 to 47 characters.

Description Use the **display bgp vpnv4 group** command to display information about a specified or all BGP VPNv4 peer groups.

Example # Display information about BGP VPNv4 peer group a for VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 group a

 BGP peer-group is a
 remote AS number not specified
 Type : external
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Configured hold timer value: 180
 Keepalive timer value: 60
 Minimum time between advertisement runs is 30 seconds
 Peer Preferred Value: 99
 No routing policy is configured
  Members:
  Peer        V   AS  MsgRcvd  MsgSent  OutQ PrefRcv Up/Down  State
  10.1.1.1    4   200   18       21     0     1      00:12:58 Established
```

Table 444 Description on the fields of the display bgp vpnv4 group command

Field	Description
BGP peer-group	Name of the BGP peer group
remote AS number	Number of the remote AS
Type	Type of the BGP peer group
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Configured hold timer value	Setting of the hold timer
Keepalive timer value	Keepalive interval
Minimum time between advertisement runs	Minimum route advertisement interval
Peer Preferred Value	Weight for the routes from the peer
No routing policy is configured	Whether the VPN instance is configured with a routing policy
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of prefixes received
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

display bgp vpnv4 network

Syntax **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **network**

View Any view

Parameter **all**: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description Use the **display bgp vpnv4 network** command to display information about BGP VPNv4 routes injected into a specified or all VPN instances.

Example # Display information about BGP VPNv4 routes injected into VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 network
  BGP Local Router ID is 1.1.1.1.
  Local AS Number is 100.
  Network          Mask            Route-policy
  10.0.0.0         255.0.0.0
```

Table 445 Description on the fields of the display bgp vpnv4 network command

Field	Description
BGP Local Router ID	Router ID of the local BGP router
Local AS Number	Number of the local AS
Network	Advertised network route
Mask	Mask of the advertised network route
Route-policy	Routing policy configured

display bgp vpnv4 paths

Syntax **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **paths** [*as-regular-expression*]

View Any view

Parameter **all**: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

as-regular-expression: Regular expression for filtering the AS path information to be displayed.

Description Use the **display bgp vpnv4 paths** command to display the BGP VPNv4 AS path information.

Example # Display the BGP VPNv4 AS path information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 paths

    Address       Hash    Refcount  MED         Path/Origin
    0x6E72D18     0       1           0           200?
    0x6E72E50     0       1           0           i
    0x6E72B78     1       1           0           ?
    0x6E72BE0     1       2           0           ?
```

Display all BGP VPNv4 AS path information.

```
<Sysname> display bgp vpnv4 all paths
    Address        Hash    Refcount  MED          Path/Origin
    0x6E72D80      4       1         0            200?
    0x6E72CB0      15      2         0            ?
```

Table 446 Description on the fields of the display bgp vpnv4 paths command

Field	Description
Address	Routing address in the local database
Hash	Hash bucket for storing routes
Refcount	Number of times that the path is referenced
MED	Metric for routes
Path/Origin	AS_PATH and origin attributes of the route, see Table 443.

display bgp vpnv4 peer

Syntax **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **peer** [*group-name* **log-info** | *ip-address* { **log-info** | **verbose** } | **verbose**]

View Any view

Parameter **all**: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

group-name: Name of the peer group, a string of 1 to 47 characters.

log-info: Displays log information.

ip-address: IP address of the peer.

verbose: Displays detailed information.

Description Use the **display bgp vpnv4 peer** command to display information about BGP VPNv4 peers.

Example # Display information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer
 BGP local router ID : 2.2.2.2
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

 Peer         V   AS  MsgRcvd  MsgSent  OutQ PrefRcv  Up/Down  State
 10.1.1.1    4   200    24       29       0       1      00:18:47 Established
```

Table 447 Description on the fields of display bgp vpnv4 vpn-instance peer

Field	Description
BGP Local router ID	Router ID of the local BGP router
local AS number	Local AS number
Total number of peers	Total number of peers
Peers in established state	Number of peers in the state of established

Table 447 Description on the fields of display bgp vpnv4 vpn-instance peer

Field	Description
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number of the peer group
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
PrefRcv	Number of received prefixes
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peers of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 peer verbose

         Peer: 10.1.1.1  Local: 2.2.2.2
         Type: EBGP link
         BGP version 4, remote router ID 10.1.1.1
         BGP current state: Established, Up for 00h19m26s
         BGP current event: KATimerExpired
         BGP last state: OpenConfirm
         Port:  Local - 179      Remote - 1025
         Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
         Received  : Active Hold Time: 180 sec
         Negotiated: Active Hold Time: 180 sec
         Peer optional capabilities:
         Peer support bgp multi-protocol extended
         Peer support bgp route refresh capability
         Address family IPv4 Unicast: advertised and received
 Received: Total 25 messages, Update messages 1
 Sent: Total 30 messages, Update messages 4
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 30 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 Peer Preferred Value: 99

 Routing policy configured:
 No routing policy is configured
```

Table 448 Description on the fields of the display bgp vpnv4 peer verbose command

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router
BGP current state	Current status of the BGP session
Up for	Duration since the peer is established
BGP current event	Current event of the BGP session
BGP last state	State that the BGP session was in before transitioning to the current status

Table 448 Description on the fields of the display bgp vpnv4 peer verbose command

Field	Description
Port	Local and remote ports of the BGP session
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Received	Total number of received messages and the number of received update messages
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Local optional capabilities
Route refresh capability has been enabled	Whether the route refresh capability is supported
Peer Preferred Value	Weight for the routes from the peer
Routing policy configured	Routing policy configured

Display all BGP VPNv4 peer information.

```
<Sysname> display bgp vpnv4 all peer

 BGP local router ID : 2.2.2.2
 Local AS number : 100
 Total number of peers : 1                 Peers in established state : 1

  Peer     V   AS  MsgRcvd  MsgSent  OutQ  PrefRcv  Up/Down   State
  1.1.1.1  4  100   51       64        0     2       00:45:16  Established
```

Table 449 Description on the fields of the display bgp vpnv4 all peer command

Field	Description
Peer	IP address of the peer
V	Version of BGP that the peer runs
AS	AS number
MsgRcvd	Number of messages received
MsgSent	Number of messages sent
OutQ	Number of messages waiting to be sent to the peer
Up/Down	Duration of the BGP session in the current state
State	Status of the peer

Display detailed information about BGP VPNv4 peer 1.1.1.1.

```
<Sysname> display bgp vpnv4 all peer 1.1.1.1 verbose
          Peer: 1.1.1.1   Local: 2.2.2.2
          Type: IBGP link
          BGP version 4, remote router ID 1.1.1.1
          BGP current state: Established, Up for 00h46m01s
          BGP current event: RecvKeepalive
          BGP last state: OpenConfirm
          Port:  Local - 1039     Remote - 179
          Configured: Active Hold Time: 180 sec   Keepalive Time:60 sec
          Received  : Active Hold Time: 180 sec
          Negotiated: Active Hold Time: 180 sec
          Peer optional capabilities:
          Peer support bgp multi-protocol extended
          Peer support bgp route refresh capability
          Address family IPv4 Unicast: advertised and received
          Address family VPNv4: advertised and received

 Received: Total 52 messages, Update messages 2
 Sent: Total 65 messages, Update messages 5
 Maximum allowed prefix number: 150000
 Threshold: 75%
 Minimum time between advertisement runs is 15 seconds
 Optional capabilities:
 Route refresh capability has been enabled
 Connect-interface has been configured
 Peer Preferred Value: 0

 Routing policy configured:
 No routing policy is configured
```

Table 450 Description on the fields of display bgp vpnv4 all peer verbose

Field	Description
Peer	IP address of the peer
Local	IP address of the local router
Type	BGP type
BGP version	Version of BGP that the peer runs
remote router ID	Router ID of the remote router
BGP current state	Current status of BGP
Up for	Duration since the peer is established
BGP current event	Current event of the peer
BGP last state	State that BGP was in before transitioning to the current status
Port	Local and remote BGP port numbers
Configured	Settings of the local timers, including the active hold interval and keepalive interval
Received	Received active hold interval
Negotiated	Negotiated active hold interval
Peer optional capabilities	Optional capabilities of the peer
Peer support bgp multi-protocol extended	The peer supports multiprotocol extension.
Peer support bgp route refresh capability	The peer supports route refresh capability.
Address family IPv4 Unicast	IPv4 unicast family capability
Address family VPNv4	IPv4 address group VPNv4 capability
Received	Total number of received messages and the number of received update messages

Table 450 Description on the fields of display bgp vpnv4 all peer verbose

Field	Description
Sent	Total number of sent messages and the number of sent update messages
Maximum allowed prefix number	Maximum number of routes that the VPN instance supports
Threshold	Threshold value
Minimum time between advertisement runs	Minimum route advertisement interval
Optional capabilities	Local optional capabilities
Route refresh capability	Whether the route refresh capability is supported
Connect-interface	Whether a source interface is configured for route update messages
Peer Preferred Value	Weight configured for routes from the peer
Routing policy configured	Routing policy configured

display bgp vpnv4 route-distinguisher routing-table

Syntax **display bgp vpnv4 route-distinguisher** *route-distinguisher* **routing-table** [*network-address* [{ *mask* | *mask-length* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13> [**no-export-subconfed** | **no-advertise** | **no-export**] * [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **different-origin-as** | **regular-expression** *as-regular-expression*]

View Any view

Parameter *route-distinguisher*: Route distinguisher (RD).

network-address: IP address of the destination segment.

mask-length: Length of the network mask, in the range 0 to 32.

mask-address: Network mask, in the format of X.X.X.X.

longer-prefixes: Matches the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays classless interdomain routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact matching.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

different-origin-as: Displays information about routes with different AS origins.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

Description Use the **display bgp vpnv4 route-distinguisher routing-table** command to display the BGP VPNv4 routing information of a specified RD.

Related command: **route-distinguisher (VPN instance view)**.

Example # Display the BGP VPNv4 routing information of RD 100:1.

```
<Sysname> display bgp vpnv4 route-distinguisher 100:1 routing-table

 Route Distinguisher: 100:1
 Total number of routes: 2

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1         (1025 /NULL )    0          100
*>i 123.1.1.1/32       1.1.1.1         (1024 /NULL )    0          100

 Total routes of vpn-instance vpn1: 5
    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1                          0          100
*>  10.1.1.0/24        0.0.0.0         (NULL /1025 )    0
*>  20.0.0.0           10.1.1.1        (NULL /1026 )    0
*>i 123.1.1.1/32       1.1.1.1                          0          100
*>  124.1.1.1/32       0.0.0.0         (NULL /1024 )    0
```

Table 451 Fields of the above output

Field	Description
Route Distinguisher	RD
Total number of routes	Total number of routes
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. For valid values, see Table 443.
Origin	Route origin codes. For valid values, see Table 443.
Network	Network address
NextHop	Address of the next hop
Label(recv/app)	Incoming/outgoing label
MED	Metric associated with the destination network
LocPrf	Local preference
Total routes of vpn-instance vpn1	Total number of routes of the specified VPN instance

Display the BGP VPNv4 routing information of RD 100:1, with the network segment address being 10.0.0.0.

```
<Sysname> display bgp vpnv4 route-distinguisher 100:1 routing-table 10.0.0.0
 255.0.0.0

 Route Distinguisher: 100:1
 Total number of routes: 1

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1         (1025 /NULL )    0          100

 Total Number of Routes: 1(vpn1)
    Network            NextHop         Label(recv/app)  MED        LocPrf

*>i 10.0.0.0           1.1.1.1                          0          100
```

Table 452 Fields of the above output

Field	Description
Route Distinguisher	RD
Total number of routes	Total number of routes
BGP Local router ID	Router ID of the local BGP router
Status codes	Route status codes. For valid values, see Table 443.
Origin	Route origin codes. For valid values, see Table 443.
Network	Network address in the BGP routing table
NextHop	Address of the next hop
Label(recv/app)	Incoming/outgoing label
MED	Metric associated with the destination network
LocPrf	Local preference
Total Number of Routes	Total number of routes of the specified VPN instance

display bgp vpnv4 routing-table label

Syntax **display bgp vpnv4** { **all** | **vpn-instance** *vpn-instance-name* } **routing-table label**

View Any view

Parameter **all**: Specifies all VPNv4 peers.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description Use the **display bgp vpnv4 routing-table label** command to display information about labeled routes in the BGP routing table.

Example # Display information about labeled routes in the BGP routing table.

```
<Sysname> display bgp vpnv4 all routing-table label

 Total number of routes from all PE: 1
 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete

 Route Distinguisher: 100:1

        Network           NextHop           In/Out Label
 *>i    123.1.1.1         1.1.1.1           NULL/1024

 Total routes of vpn-instance vpn1: 4

        Network           NextHop           In/Out Label
 *>     10.1.1.0          0.0.0.0           1025/NULL
 *>     20.0.0.0          0.0.0.0           1026/NULL
 *>i    123.1.1.1         1.1.1.1           NULL/1024
 *>     124.1.1.1         0.0.0.0           1024/NULL
```

Table 453 Description on the fields of display bgp vpnv4 routing-table label

Field	Description
Total number of routes from all PE	Total number of routes from all PEs
BGP Local router ID	Router ID of the local BGP router
Status	Route status codes. For valid values, see Table 443.
Origin	Route origin codes. For valid values, see Table 443.
Route Distinguisher	RD
Network	Network address
NextHop	Address of the next hop
In/Out Label	Incoming/outgoing label. exp-null indicates an explicit null label.
Total routes of vpn-instance vpn1	Total number of routes from the specified VPN instance

display bgp vpnv4 vpn-instance routing-table

Syntax **display bgp vpnv4 vpn-instance** *vpn-instance-name* **routing-table** [*network-address* [{ *mask-length* | *mask-address* } [**longer-prefixes**]] | **as-path-acl** *as-path-acl-number* | **cidr** | **community** [*aa:nn*]&<1-13>[**no-export-subconfed** | **no-advertise** | **no-export**]* [**whole-match**] | **community-list** { *basic-community-list-number* [**whole-match**] | *adv-community-list-number* }&<1-16> | **dampened** | **dampening parameter** | **different-origin-as** | **flap-info** [**as-path-acl** *as-path-acl-number* | *network-address* [*mask* [**longer-match**] | *mask-length* [**longer-match**]] | **regular-expression** *as-regular-expression*] | **peer** *ip-address* { **advertised-routes** | **received-routes** } | **regular-expression** *as-regular-expression* | **statistic**]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

network-address: IP address of the destination segment.

mask-length: Length of the network mask, in the range 0 to 32.

mask-address: Network mask, in the format of X.X.X.X.

longer-prefixes: Specifies to match the longest prefix.

as-path-acl *as-path-acl-number*: Filters routing information using the specified AS_PATH list. The *as-path-acl-number* argument ranges from 1 to 256.

cidr: Displays classless interdomain routing (CIDR) information.

community: Displays routing information of the specified BGP community in the routing table.

aa:nn&<1-13>: Community number. Both the *aa* and *nn* parameters range from 0 to 65535. &<1-13> means that you can enter the parameter combination up to 13 times.

no-export-subconfed: A route with this attribute is neither advertised out of the local AS, nor advertised to the other sub-ASs in the confederation.

no-advertise: A route with this attribute is not advertised to any other BGP peer.

no-export: A route with this attribute is not advertised out of the local AS or, If existing, confederation. However, it is advertised to the other sub-ASs in the confederation.

whole-match: Performs exact match.

community-list: Displays routing information of the specified BGP community list.

basic-community-list-number: Basic community list number, in the range 1 to 99.

adv-community-list-number: Advanced community list number, in the range 100 to 199.

&<1-16>: Specifies that the argument before it can be entered up to 16 times.

dampened: Displays information about dampened BGP VPNv4 routes.

dampening parameter: Displays information about configured BGP VPNv4 route dampening parameters.

different-origin-as: Displays information about routes with different AS origins.

flap-info: Displays BGP VPNv4 route flap statistics.

longer-match: Displays flap statistics for routes with masks longer than that specified by the *network-address* { *mask* | *mask-length* } combination.

peer *ip-address*: Specifies a peer by its IP address.

advertised-routes: Displays routing information sent to the specified peer.

received-routes: Displays routing information received from the specified peer.

regular-expression *as-regular-expression*: Displays routing information matching the specified AS regular expression.

statistic: Displays BGP VPNv4 route statistics.

Description Use the **display bgp vpnv4 vpn-instance routing-table** command to display the BGP VPNv4 routing information of a specified VPN instance.

Example # Display the BGP VPNv4 routing information of VPN instance vpn1.

```
<Sysname> display bgp vpnv4 vpn-instance vpn1 routing-table

 Total Number of Routes: 5

 BGP Local router ID is 2.2.2.2
 Status codes: * - valid, > - best, d - damped,
               h - history,  i - internal, s - suppressed, S - Stale
               Origin : i - IGP, e - EGP, ? - incomplete
 Network            NextHop         MED        LocPrf    PrefVal Path/Ogn

 *>i 10.0.0.0       1.1.1.1         0          100        0       i
 *>  10.1.1.0/24    0.0.0.0         0                     0       ?
 *>  20.0.0.0       10.1.1.1        0                     99      200?
 *>i 123.1.1.1/32   1.1.1.1         0          100        0       ?
 *>  124.1.1.1/32   0.0.0.0         0                     0       ?
```

Table 454 Fields of display bgp vpnv4 vpn-instance routing-table

Field	Description
Total Number of Routes	Total number of routes
BGP Local router ID	ID of the BGP-enabled local router
Status codes	Route status codes. For valid values, see Table 443.
Origin	Route origin codes. For valid values, see Table 443.
Network	Network address in the BGP routing table

Table 454 Fields of display bgp vpnv4 vpn-instance routing-table

Field	Description
NextHop	Address of the next hop
MED	Metric associated with the destination network
LocPrf	Local preference
PrefVal	Preferred value of the protocol
Path/Ogn	AS_PATH attribute/route origin of the route, see Table 443.

display fib statistics vpn-instance

Syntax **display fib statistics vpn-instance**

View Any view

Parameter None

Description Use the **display fib statistics vpn-instance** command to display statistics about the VPN instance forwarding table.

Example # Display statistics about the VPN instance forwarding table.

```
<Sysname> display fib statistics vpn-instance
Route Entry Count              : 10
```

Table 455 Description on the fields of display fib statistics vpn-instance

Field	Description
Route Entry Count	Total route number of all created VPN instances

display fib vpn-instance

Syntax **display fib vpn-instance** *vpn-instance-name* [**include** *string*]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

include *string*: Displays only information that includes the specified string. The *string* argument is case-sensitive and consists of 1 to 256 characters.

Description Use the **display fib vpn-instance** command to display information about the forwarding information base (FIB) of a VPN instance.

Example # Display information about the FIB of VPN instance vpn1.

```
<Sysname> display fib vpn-instance vpn1
FIB Table For vpn1:
 Total number of Routes : 2
```

```
Destination/Mask    OutInterface                 InnerLabel     Token
66.1.1.1/32         InLoopBack0                  NULL           invalid
66.1.1.0/24         Ethernet1/0                  NULL           invalid
```

Table 456 Description on the fields of the display fib vpn-instance command

Field	Description
FIB Table For vpn1	FIB information about VPN instance vpn1
Total number of Routes	Total number of routes
Destination/Mask	Forwarding destination address and mask of the VPN instance
OutInterface	Outbound interface of the VPN instance
InnerLabel	Inner label
Token	Token

display ip vpn-instance

Syntax **display ip vpn-instance** [**instance-name** *vpn-instance-name*]

View Any view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

Description Use the **display ip vpn-instance** command to display information about a VPN instance or all VPN instances.

If you do not specify any parameter, the command displays brief information about all VPN instances.

Example # Display information about all VPN instances.

```
<Sysname> display ip vpn-instance
  Total VPN-Instances configured : 2

  VPN-Instance Name      RD           Create Time
  vpn1                  22:1         2003/10/13 09:32:45
  vpn2                  33:3         2003/10/13 09:42:59
```

Table 457 Description on the fields of the display ip vpn-instance command

Field	Description
VPN-Instance Name	Name of the VPN instance
RD	RD of the VPN instance
Create Time	Time when the VPN instance was created

Display detailed information about a VPN instance.

```
<Sysname> display ip vpn-instance instance-name vpn1
  VPN-Instance Name and ID : vpn1, 1
  Create time : 2006/04/08 13:01:30
  Up time : 0 days, 00 hours, 11 minutes and 42 seconds
  Route Distinguisher : 22:1
  Export VPN Targets :  3:3 5:5
```

```
Import VPN Targets :  4:4 5:5
Import Route Policy : poly-1
Description : This is vpn1
Maximum number of Routes : 500
Interfaces :  Ethernet1/0
```

Table 458 Description on the fields of display ip vpn-instance instance-name

Field	Description
VPN-Instance Name and ID	Name and ID of the VPN instance
CreateTime	Time when the VPN instance was created
Up time	Duration of the VPN instance
Route Distinguisher	RD of the VPN instance
Export VPN Targets	Export target attribute of the VPN instance
Import VPN Targets	Import target attribute of the VPN instance
Import Route Policy	Import routing policy of the VPN instance
Description	Description of the VPN instance
Maximum number of Routes	Maximum number of routes of the VPN instance
Interfaces	Interface to which the VPN instance is bound

display ospf sham-link

Syntax **display ospf** [*process-id*] **sham-link** [**area** *area-id*]

View Any view

Parameter *process-id*: OSPF process ID, in the range 1 to 65535.

area-id: OSPF area ID. It can be an integer in the range 0 to 4294967295 or in the format of an IPv4 address.

Description Use the **display ospf sham-link** command to display information about sham links.

With neither process ID nor area ID specified, the command displays information about all configured sham links.

Related command: **sham-link**.

Example # Display information about all OSPF sham links.

```
<Sysname> display ospf sham-link
          OSPF Process 100 with Router ID 100.1.1.2
 Sham Link:
 Area        RouterId     Source-IP     Destination-IP  State Cost
 0.0.0.1     100.1.1.2    3.3.3.3       5.5.5.5         P-2-P 10
```

Table 459 Description on the fields of the display ospf sham-link command

Field	Description
Area	OSPF area to which the sham link belongs

Table 459 Description on the fields of the display ospf sham-link command

Field	Description
RouterId	Router ID of the sham link
Source-IP	Source IP address of the sham link
Destination-IP	Destination IP address of the sham link
State	Status of the sham link interface
Cost	Cost of the sham link

Display information about OSPF sham links in area 1.

```
<Sysname> display ospf sham-link area 1
          OSPF Process 100 with Router ID 100.1.1.2
  Sham-Link: 3.3.3.3 --> 5.5.5.5
  Neighbour State: Full
  Area: 0.0.0.1
  Cost: 10  State: P-2-P, Type: Sham
  Timers: Hello 10 , Dead 40 , Retransmit 5 , Transmit Delay 1
```

Table 460 Description on the fields of the display ospf sham-link area command

Field	Description
Sham-Link	Sham link expressed in the format of source IP address to destination IP address
Neighbor State	Status of the sham link neighbor
Area	Destination IP address of the sham link
Cost	Cost of the sham link
State	Status of the sham link
Type	Type of the sham link
Timers	Timers of the sham link

display tunnel-policy

Syntax **display tunnel-policy** { **all** | **policy-name** *tunnel-policy-name* }

View Any view

Parameter **all**: Specifies all tunneling policies.

tunnel-policy-name: Name of a tunneling policy, a string of 1 to 19 characters.

Description Use the **display tunnel-policy** command to display information about a tunneling policy or all tunneling policies.

Related command: **tunnel-policy**, **tunnel select-seq load-balance-number**.

Example # Display all tunneling policies.

```
<Sysname>display tunnel-policy all
Tunnel Policy Name   Select-Seq       Load balance No
-----------------------------------------------------
```

```
t                    LSP              1
aaa                  LSP CR-LSP GRE   1
bbb                  LSP              1
```

Display tunneling policy aaa.

```
<Sysname>display tunnel-policy policy-name aaa
Tunnel Policy Name   Select-Seq       Load balance No
------------------------------------------------------
aaa                  LSP CR-LSP GRE   1
```

Table 461 Description on the fields of the display tunnel-policy command

Field	Description
Tunnel Policy Name	Name of the tunneling policy
Select-Seq	preference order for tunnel selection
Load balance No	Number of tunnels for load balancing

domain-id

Syntax **domain-id** *domain-id* [**secondary**]

undo domain-id [*domain-id*]

View OSPF view

Parameter *domain-id*: OSPF domain ID, in integer or dotted decimal notation. If it is in integer, it ranges from 0 to 4,294,967,295.

secondary: Uses the domain ID as secondary. With this keyword not specified, the domain ID configured is primary.

Description Use the **domain-id** command to configure an OSPF domain ID.

Use the **undo domain-id** command to restore the default.

By default, the OSPF domain ID is 0.

With no parameter specified, the **undo domain-id** command deletes the primary domain ID.

Usually, routes injected from PEs are advertised as External-LSAs. However, routes to different destinations in the same OSPF domain must be advertised as Type-3 LSAs. Therefore, using the same domain ID for an OSPF domain is required.

Example # Configure the OSPF domain ID.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] domain-id 234
```

export route-policy

Syntax **export route-policy** *route-policy*

undo export route-policy

View VPN instance view

Parameter *route-policy*: Name of the export routing policy for the VPN instance, a string of 1 to 19 characters.

Description Use the **export route-policy** command to apply an export routing policy to a VPN instance.

Use the **undo export route-policy** command to remove the application.

You can configure an export routing policy when a finer control on the VPN instance routes to be redistributed is required, that is, when the control provided by the extended community attribute is not enough. An export routing policy may deny routes that are permitted by the export target attribute.

By default, all VPN instance routes permitted by the export target attribute can be redistributed.

Example # Apply export routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] export route-policy poly-1
```

filter-policy export (BGP-VPNv4 subaddress family view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **export** [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

undo filter-policy export [**direct** | **isis** *process-id* | **ospf** *process-id* | **rip** *process-id* | **static**]

View BGP-VPNv4 subaddress family view

Parameter *acl-number*: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

direct: Filters direct routes to be advertised.

isis *process-id*: Filters ISIS routes to be advertised that are from a specified ISIS process. The *process-id* argument is in the range 1 to 65535.

ospf *process-id*: Filters OSPF routes to be advertised that are from a specified OSPF process. The *process-id* argument is in the range 1 to 65535.

rip *process-id*: Filters RIP routes to be advertised that are from a specified RIP process. The *process-id* argument is in the range 1 to 65535.

static: Filters static routes to be advertised.

Description Use the **filter-policy export** command to specify to filter all or certain types of routes to be advertised.

Use the **undo filter-policy export** command to remove the configuration.

If you specify no routing protocol parameters for the **filter-policy export** command, all routes to be advertised will be filtered.

By default, MP-BGP does not filter routes to be advertised.

Only routes that survive the filtering are advertised by MP-BGP.

Example # In BGP-VPNv4 subaddress family view, specify to filter routes to be advertised by MP-BGP using ACL 2555.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] filter-policy 2555 export
```

filter-policy import (BGP-VPNv4 subaddress family view)

Syntax **filter-policy** { *acl-number* | **ip-prefix** *ip-prefix-name* } **import**

undo filter-policy import

View BGP-VPNv4 subaddress family view

Parameter *acl-number*: IP ACL number, in the range 2000 to 3999.

ip-prefix-name: IP address prefix list name, a string of 1 to 19 characters.

Description Use the **filter-policy import** command to specify to filter received routes.

Use the **undo filter-policy import** command to remove the configuration.

By default, received routes are not filtered.

Only routes that survive the filtering are added into the BGP routing table.

Example # In BGP-VPNv4 subaddress family view, specify to use ACL 2255 to filter received routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] filter-policy 2255 import
```

import route-policy

Syntax **import route-policy** *route-policy*

undo import route-policy

View VPN instance view

Parameter *route-policy*: Name of the import routing policy for the VPN instance, a string of 1 to 19 characters.

Description Use the **import route-policy** command to apply an import routing policy to a VPN instance.

Use the **undo import route-policy** command to remove the application.

You can configure an import routing policy when a finer control on the routes to be redistributed into a VPN instance is required, that is, when the control provided by the extended community attributes is not enough. An import routing policy may deny routes that are permitted by the import target attribute.

By default, all routes permitted by the import target attribute can be redistributed into the VPN instance.

Example # Apply import routing policy poly-1 to VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] import route-policy poly-1
```

ip binding vpn-instance

Syntax **ip binding vpn-instance** *vpn-instance-name*

undo ip binding vpn-instance *vpn-instance-name*

View Interface view

Parameter *vpn-instance-name*: Name of the VPN instance to be associated, a case-insensitive string of 1 to 31 characters.

Description Use the **ip binding vpn-instance** command to associate an interface with a VPN instance.

Use the **undo ip binding vpn-instance** command to remove the association.

By default, an interface is associated with no VPN instance; it belongs to the public network.

When configured on an interface, the **ip binding vpn-instance** command clears the IP address of the interface. Therefore, you must re-configure the IP address of the interface after configuring the command.

Example # Associate interface Ethernet1/0 with VPN instance vpn1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Etherne1/0] ip binding vpn-instance vpn1
```

ip vpn-instance

Syntax **ip vpn-instance** *vpn-instance-name*

undo ip vpn-instance *vpn-instance-name*

View System view

Parameter *vpn-instance-name*: Name for the VPN instance, a case-sensitive string of 1 to 31 characters.

Description Use the **ip vpn-instance** command to create a VPN instance and enter VPN instance view.

Use the **undo ip vpn-instance** command to delete a VPN instance.

A VPN instance takes effect only after you configure an RD for it.

Related command: **route-distinguisher (VPN instance view)**.

Example # Create a VPN instance named vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1]
```

ipv4-family

Syntax **ipv4-family** { **vpnv4** | **vpn-instance** *vpn-instance-name* }

undo ipv4-family { **vpnv4** | **vpn-instance** *vpn-instance-name* }

View BGP view

Parameter **vpnv4**: Enters BGP-VPNv4 subaddress family view.

vpn-instance *vpn-instance-name*: Associates a VPN instance with an IPv4 address family and enter BGP VPN instance view. The *vpn-instance-name* argument is a string of 1 to 31 characters.

Description Use the **ipv4-family** command to enter BGP-VPNv4 subaddress family view or BGP VPN instance view.

Use the **undo ipv4-family** command to remove all configurations performed in either of the two views.

Before entering BGP VPN instance view, you must create the VPN instance.

Example # Enter BGP-VPNv4 subaddress family view.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4]
```

Associate VPN instance vpn1 with an IPv4 address family and enter BGP VPN instance view.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] quit
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpn-instance vpn1
[Sysname-bgp-vpn1]
```

peer advertise-community (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **advertise-community**

undo peer { *group-name* | *ip-address* } **advertise-community**

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer advertise-community** command to specify to advertise community attributes to a peer or peer group.

Use the **undo peer advertise-community** command to remove the configuration.

By default, no community attributes are advertised to any peer or peer group.

Example # In BGP-VPNv4 subaddress family view, specify to advertise community attributes to peer 3.3.3.3.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 3.3.3.3 advertise-community
```

peer allow-as-loop

Syntax **peer** { *group-name* | *ip-address* } **allow-as-loop** [*number*]

undo peer { *group-name* | *ip-address* } **allow-as-loop**

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

number: Maximum number that the local AS number can appear repeatedly in the AS-PATH attribute. It ranges from 1 to 10 and defaults to 1.

Description Use the **peer allow-as-loop** command to allow the local AS number to appear in the AS-PATH attribute of a received route and to set the allowed maximum number of repetitions.

Use the **undo peer allow-as-loop** command to remove the configuration.

Example # In BGP-VPNv4 subaddress family view, allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 allow-as-loop 2
```

In BGP-L2VPN address family view, allow the local AS number to appear repeatedly in the AS-PATH attribute of a route received from peer 1.1.1.1 for up to twice.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 allow-as-loop 2
```

peer as-path-acl (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **as-path-acl** *aspath-filter-number* { **import** | **export** }

undo peer { *group-name* | *ip-address* } **as-path-acl** *aspath-filter-number* { **import** | **export** }

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

aspath-acl-number: AS_PATH filtering list number, in the range 1 to 256.

import: Filters the received routes.

export: Filters the routes to be advertised.

Description Use the **peer as-path-acl** command to specify to filter routes received from or to be advertised to a specified peer or peer group based on an AS_PATH list.

Use the **undo peer as-path-acl** command to remove the configuration.

By default, no AS filtering list is applied to a peer or peer group.

Example # In BGP-VPNv4 subaddress family view, apply AS filtering list 3 to routes advertised by peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test as-path-acl 3 export
```

peer default-route-advertise vpn-instance

Syntax **peer** { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*

undo peer { *group-name* | *ip-address* } **default-route-advertise vpn-instance** *vpn-instance-name*

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

vpn-instance-name: Name of the VPN instance, a string of 1 to 31 characters.

Description Use the **peer default-route-advertise vpn-instance** command to specify to advertise all default routes of a VPN instance to a peer or peer group.

Use the **undo peer default-route-advertise vpn-instance** command to remove the configuration.

By default, no default route is advertised to a peer or peer group.

Related command: **peer upe**.

Example # In BGP-VPNv4 subaddress family view, specify to advertise default routes of VPN instance vpn1 to peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 enable
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 upe
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 default-route-advertise vpn-inst
ance vpn1
```

peer enable

Syntax **peer** { *group-name* | *ip-address* } **enable**

undo peer { *group-name* | *ip-address* } **enable**

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer enable** command to enable a peer or peer group for an address family and enable the exchange of BGP routing information of the address family.

Use the **undo peer enable** command to disable the capability.

By default, only IPv4 routing information is exchanged between BGP peers/peer groups.

Example # Configure peer 1.1.1.1 and enable the peer for the BGP-VPNv4 subaddress family.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 enable
```

Configure peer 1.1.1.1 and enable the peer for the BGP-L2VPN address family.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 1.1.1.1 as-number 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 enable
```

peer filter-policy (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **filter-policy** *acl-number* { **export** | **import** }

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

acl-number: ACL number, in the range 2000 to 3999.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description Use the **peer filter-policy** command to apply a filtering policy to a peer or peer group.

Use the **undo peer filter-policy** command to remove the configuration.

By default, no filtering policy is applied to a peer or peer group.

Related command: **peer as-path-acl (BGP-VPNv4 subaddress family view)**.

Example # Apply a filtering policy to filter the received routes of a peer group.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test filter-policy 2003 import
```

peer group

Syntax **peer** *ip-address* **group** *group-name*

undo peer *ip-address* **group** *group-name*

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer group** command to add a peer into an existing peer group.

Use the **undo peer group** command to remove a peer from a peer group.

Example # In BGP-VPNv4 subaddress family view, add peer 1.1.1.1 into peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
```

```
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 group test
```

In BGP-L2VPN address family view, add peer 1.1.1.1 into peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] group test external
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer 1.1.1.1 group test
```

peer ip-prefix (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **ip-prefix** *prefix-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **ip-prefix** *prefix-name* { **export** | **import** }

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

prefix-name: Name of the IP prefix list, a string of 1 to 19 characters.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description Use the **peer ip-prefix** command to apply a route filtering policy based on IP prefix list to a peer or peer group.

Use the **undo peer ip-prefix** command to remove the configuration.

By default, no route filtering policy based on IP prefix list is applied to a peer or peer group.

Example # In BGP-VPNv4 subaddress family view, specify to filter the received routes of a peer group using IP prefix list list1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer group1 ip-prefix list1 import
```

peer label-route-capability (BGP view/BGP VPN instance view)

Syntax **peer** { *group-name* | *ip-address* } **label-route-capability**

undo peer { *group-name* | *ip-address* } **label-route-capability**

View BGP view/BGP VPN instance view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer label-route-capability** command to enable the exchange of labeled routes with an IPv4 peer or peer group.

Use the **undo peer label-route-capability** command to disable the capability.

By default, the device does not advertise labeled routes to an IPv4 peer.

According to the networking scheme, the **peer label-route-capability** command enables the exchange of labeled IPv4 routes with:

- ASBR PEs in the same AS.
- PEs in the same AS.
- the peer ASBR PE.

Example # Specify to exchange labeled IPv4 routes with peer 2.2.2.2.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] peer 2.2.2.2 label-route-capability
```

peer next-hop-invariable (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **next-hop-invariable**

undo peer { *group-name* | *ip-address* } **next-hop-invariable**

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer next-hop-invariable** command to configure the device not to change the next hop of a route when advertising it to an EBGP peer.

Use the **undo peer next-hop-invariable** command to restore the default.

By default, a device uses its address as the next hop when advertising a route to its EBGP peer.

Related command:. **peer ebgp-max-hop (BGP/BGP-VPN instance view) on page 991**

Example # In BGP-VPNv4 subaddress family view, configure the device not to change the next hop of a route when advertising it to EBGP peer 1.1.1.1.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 next-hop-invariable
```

peer next-hop-local

Syntax **peer** { *group-name* | *ip-address* } **next-hop-local**

undo peer { *group-name* | *ip-address* } **next-hop-local**

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer next-hop-local** command to configure the device to use the local address as the next hop of a route when advertising it to a peer or peer group.

Use the **undo peer next-hop-local** command to remove the configuration.

Example # In BGP-VPNv4 subaddress family view, configure the device to use the local address as the next hop of a route when advertising it to peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test next-hop-local
```

In BGP-L2VPN address family view, configure the device to use the local address as the next hop of a route when advertising it to peer group test.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer test next-hop-local
```

peer public-as-only (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **public-as-only**

undo peer { *group-name* | *ip-address* } **public-as-only**

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer public-as-only** command to make outbound BGP updates carry no private AS numbers.

Use the **undo peer public-as-only** command to make outbound BGP updates carry private AS numbers.

By default, a BGP update carries private AS numbers.

If a BGP update to be sent carries any public AS number, this command does not take effect. The private AS number ranges from 64512 to 65535.

Example # In BGP-VPNv4 subaddress family view, configure the device to make BGP updates to be sent to peer group test carry no private AS numbers.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test public-as-only
```

peer reflect-client

Syntax **peer** { *group-name* | *ip-address* } **reflect-client**

undo peer { *group-name* | *ip-address* } **reflect-client**

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer reflect-client** command to configure the local device to be a route reflector (RR) and set a peer or peer group as the client of the RR.

Use the **undo peer reflect-client** command to remove the configuration.

By default, no RR or RR client is configured.

Example # In BGP-VPNv4 subaddress family view, configure the local device to be an RR and set peer group test as the client of the RR.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test reflect-client
```

In BGP-L2VPN address family view, configure the local device to be an RR and set peer group test as the client of the RR.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] peer test reflect-client
```

peer route-policy (BGP-VPNv4 subaddress family view)

Syntax **peer** { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

undo peer { *group-name* | *ip-address* } **route-policy** *route-policy-name* { **export** | **import** }

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

route-policy-name: Name of the routing policy, a string of 1 to 19 characters.

export: Filters the routes to be advertised.

import: Filters the received routes.

Description Use the **peer route-policy** command to apply a routing policy to a peer or peer group.

Use the **undo peer route-policy** command to remove the application.

By default, no routing policy is applied to a peer or peer group.

Example # In BGP-VPNv4 subaddress family view, apply routing policy test-policy to peer group test to filter the received routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer test route-policy test-policy import
```

peer upe

Syntax **peer** { *group-name* | *ip-address* } **upe**

undo peer { *group-name* | *ip-address* } **upe**

View BGP-VPNv4 subaddress family view

Parameter *group-name*: Name of the peer group, a string of 1 to 47 characters.

ip-address: IP address of the peer.

Description Use the **peer upe** command to configure a BGP peer or peer group as an HoVPN UPE for a BGP-VPNv4 subaddress family.

Use the **undo peer upe** command to remove the configuration.

UPE is a kind of special VPNv4 peer. It accepts only one default route for each related VPN instance on an SPE, rather than common VPNv4 routes. An SPE is a common VPN peer.

Example # Configure peer 1.1.1.1 as a UPE.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] peer 1.1.1.1 upe
```

policy vpn-target

Syntax **policy vpn-target**

undo policy vpn-target

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter None

Description Use the **policy vpn-target** command to enable VPN target filtering for received VPNv4 routes.

Use the **undo policy vpn-target** command to disable the filtering, permitting all VPNv4 routes.

Only VPNv4 routes with export route target attributes matching the local import route target attributes are added into the routing table.

By default, the VPN target filtering function is enabled for received VPNv4 routes.

The command applies to inter-provider VPN option B schemes.

Example # In BGP-VPNv4 subaddress family view, enable VPN target filtering for received VPNv4 routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] policy vpn-target
```

In BGP-L2VPN address family view, enable VPN target filtering for received VPNv4 routes.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] policy vpn-target
```

reflect between-clients

Syntax **reflect between-clients**

undo reflect between-clients

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter None

Description Use the **reflect between-clients** command to enable route reflection between clients.

Use the **undo reflect between-clients** command to disable the function.

By default, route reflection between clients is enabled.

If fully meshed interconnections exist between the clients, route reflection is not required. Otherwise, an RR is required for routes to be reflected from one client to every other client.

Example # In BGP-VPNv4 subaddress family view, disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] undo reflect between-clients
```

In BGP-L2VPN address family view, disable route reflection between clients.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] undo reflect between-clients
```

reflector culster-id

Syntax **reflector cluster-id** { *cluster-id* | *ip-address* }

undo reflector cluster-id

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *cluster-id*: Cluster ID of the route reflector (RR), in the range 1 to 4294967295.

ip-address: IP address of the peer, which is to be used as the cluster ID of the RR.

Description Use the **reflector cluster-id** command to specify a cluster ID for an RR.

Use the **undo reflector cluster-id** command to remove the cluster ID.

By default, the cluster ID is the router ID of an RR in the cluster.

Generally, a cluster contains only one RR, in which case the router ID of the RR is used for identifying the cluster. Setting multiple RRs can improve the network reliability. When there is more than one RR in a cluster, use the **reflector cluster-id** command to configure the same cluster ID for all RRs in the cluster.

Example # In BGP-VPNv4 subaddress family view, configure the local router as an RR of a cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] reflector cluster-id 50
```

In BGP-L2VPN address family view, configure the local router as an RR of a cluster.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] reflector cluster-id 50
```

refresh bgp vpn-instance

Syntax **refresh bgp vpn-instance** *vpn-instance-name* { *ip-address* | **all** | **external** | **group** *group-name* } { **export** | **import** }

View User view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: Performs a soft reset of the BGP connection with a BGP peer identified by this IP address.

all: Performs a soft reset of all BGP VPN instance connections.

external: Performs a soft reset of EBGP sessions.

group *group-name*: Performs a soft reset of the connections with a BGP peer group identified by this name. The *group-name* argument is a string of 1 to 47 characters.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description Use the **refresh bgp vpn-instance** command to perform a soft reset of BGP connections in a VPN instance.

Example # Perform a soft reset of all BGP connections in VPN instance vpn1 in the inbound direction to make new configurations take effect.

```
<Sysname> refresh bgp vpn-instance vpn1 all import
```

refresh bgp vpnv4

Syntax **refresh bgp vpnv4** { *ip-address* | **all** | **external** | **group** *group-name* | **internal** } { **export** | **import** }

View User view

Parameter *ip-address*: Performs a soft reset of the BGP VPNv4 connection with a BGP peer identified by this IP address.

all: Performs a soft reset of all BGP VPNv4 connections.

external: Performs a soft reset of EBGP sessions.

group *group-name*: Performs a soft reset of the VPNv4 connections with a BGP peer group identified by this name.

internal: Performs a soft reset of IBGP sessions.

export: Performs a soft reset in the outbound direction.

import: Performs a soft reset in the inbound direction.

Description Use the **refresh bgp vpnv4** command to perform a soft reset of BGP VPNv4 connections.

Example # Perform a soft reset of all BGP VPNv4 connections in the inbound direction to make new configurations take effect.

```
<Sysname> refresh bgp vpnv4 all import
```

reset bgp vpn-instance

Syntax **reset bgp vpn-instance** *vpn-instance-name* { *as-number* | *ip-address* | **all** | **external** | **group** *group-name* }

View User view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

as-number: Resets BGP connections with the peers in an AS identified by this number. This argument is in the range 1 to 65535.

ip-address: Resets the connection with a BGP peer identified by this IP address.

group *group-name*: Resets the connections with a BGP peer group identified by this name. The *group-name* argument is a string of 1 to 47 characters.

all: Resets all BGP connections.

external: Resets EBGP sessions.

Description Use the **reset bgp vpn-instance** command to reset the BGP connections of a VPN instance.

Example # Reset all BGP connections of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 all
```

reset bgp vpn-instance dampening

Syntax **reset bgp vpn-instance** *vpn-instance-name* **dampening** [*network-address* [*mask* | *mask-length*]]

View User view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

dampening: Specifies route flap dampening information.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

Description Use the **reset bgp vpn-instance dampening** command to clear the route flap dampening information of a VPN instance.

Example # Clear the route flap dampening information of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 dampening
```

reset bgp vpn-instance flap-info

Syntax **reset bgp vpn-instance** *vpn-instance-name ip-address* **flap-info**

reset bgp vpn-instance *vpn-instance-name* **flap-info** [*ip-address* [*mask* | *mask-length*] | **as-path-acl** *as-path-acl-number* | **regexp** *as-path-regexp*]

View User view

Parameter *vpn-instance-name*: Name of the VPN instance, a string of 1 to 31 characters.

ip-address: IP address of the BGP peer.

mask: Network mask, in the format of X.X.X.X.

mask-length: Length of the network mask, in the range 0 to 32.

as-path-acl-number: Number of the AS_PATH list, in the range 1 to 256.

as-path-regexp: AS_PATH regular expression.

Description Use the **reset bgp vpn-instance flap-info** command to clear the route flap history information about BGP peers of a VPN instance.

Example # Clear route flap history information about BGP peer 2.2.2.2 of VPN instance vpn1.

```
<Sysname> reset bgp vpn-instance vpn1 2.2.2.2 flap-info
```

reset bgp vpnv4

Syntax **reset bgp vpnv4** { *as-number* | *ip-address* | **all** | **external** | **internal** | **group** *group-name* }

View User view

Parameter *as-number*: Resets VPNv4 connections with the peers in an AS identified by this number.

ip-address: Resets the VPNv4 connection with a BGP peer identified by this IP address.

group-name: Resets the VPNv4 connections with a BGP peer group identified by this name.

all: Resets all BGP VPNv4 connections.

external: Resets EBGP sessions of VPNv4 connections.

internal: Resets IBGP sessions of VPNv4 connections.

Description Use the **reset bgp vpnv4** command to reset BGP VPNv4 connections.

Example # Reset all BGP VPNv4 connections to make new configurations take effect.

```
<Sysname> reset bgp vpnv4 all
```

route-distinguisher (VPN instance view)

Syntax **route-distinguisher** *route-distinguisher*

View VPN instance view

Parameter *route-distinguisher*: Route distinguisher (RD) for the VPN instance, a string of 3 to 21 characters in either of the following two formats:

- 16-bit AS number: 32-bit user-defined number. For example, 101:3.

- 32-bit IP address: 16-bit user-defined number. For example, 192.168.122.15:1.

Description Use the **route-distinguisher** command to configure a route distinguisher (RD) for a VPN instance.

An RD is used to create the routing and forwarding table of a VPN. By prefixing an RD to an IPv4 prefix, you get a VPN IPv4 prefix unique globally.

- *No RD is configured by default; you must configure an RD for each VPN instance.*
- *A VPN instance takes effect only after you configure an RD for it.*
- *Once you configure an RD for a VPN, you cannot remove the association.*
- *You cannot change an RD directly; you can only delete the VPN instance, and then re-create the VPN instance and re-configure a new RD.*

Example # Configure the RD of VPN instance vpn1.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 22:1
```

route-tag

Syntax **route-tag** *tag-value*

undo route-tag

View OSPF view

Parameter *tag-value*: Tag for identifying injected VPN routes, in the range 0 to 4294967295.

Description Use the **route-tag** command to configure the tag for identifying injected VPN routes.

Use the **undo route-tag** command to restore the default.

The first two octets of the default tag is always 0xD000, while the last two octets is the AS number of the local BGP. For example, if the local BGP AS number is 100, the default tag is 3489661028 in decimal.

An OSPF instance-related VPN instance on a PE is usually configured with a VPN route tag, which must be included in Type 5/7 LSAs. PEs in the same AS are recommended to have the same route tag. The route tag is local significant and can be configured and take effect on only PEs receiving BGP routes and generating OSPF LSAs; it is not transferred in any BGP extended community attribute. Different OSPF processes can have the same route tag.

Tags configured with different commands have different priorities:

- A tag configured with the **import-route** command has the highest priority.

- A tag configured with the **route-tag** command has the second highest priority.
- A tag configured with the **default tag** command has the lowest priority.

A received Type 5 or Type 7 LSA is neglected in route calculation if its tag is the same as the local one.

*A configured route tag takes effect after you issue the **reset ospf** command.*

Related command: **import-route (OSPF view)** on page 1136.

Example # Configure the route tag for OSPF process 100 as 100.

```
<Sysname> system-view
[Sysname] ospf 100
[Sysname-ospf-100] route-tag 100
```

routing-table limit

Syntax **routing-table limit** *number* { *warn-threshold* | **simply-alert** }

undo routing-table limit

View VPN instance view

Parameter *number*: Maximum number of routes for the VPN instance to support, in the range 1 to 1024 for MSR20 and MSR30 series routers and 1 to 2048 for MSR50 series routers.

warn-threshold: Threshold for rejecting new routes. It is expressed in the percentage of the specified maximum number of routes for the VPN instance. It ranges from 1 to 100.

simply-alert: Specifies that when the maximum number of routes exceeds the threshold, the system still accepts routes and generates only a SYSLOG error message.

Description Use the **routing-table limit** command to limit the maximum number of routes in a VPN instance, preventing too many routes from being accepted a PE.

Use he **undo routing-table limit** command to restore the default.

The default maximum number of routes that a VPN instance supports varies by device.

Example # Specify that VPN instance vpn1 can receive up to 1,000 routes, and can receive new routes after the threshold is exceeded.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] route-distinguisher 100:1
[Sysname-vpn-instance-vpn1] routing-table limit 1000 simply-alert
```

rr-filter

Syntax **rr-filter** *extended-community-list-number*

undo rr-filter

View BGP-VPNv4 subaddress family view/BGP-L2VPN address family view

Parameter *extended-community-list-number*: Number of the extended community list supported by the RR group, in the range 1 to 199.

Description Use the **rr-filter** command to create an RR reflection policy.

Use the **undo rr-filter** command to disable the function.

Only IBGP routes whose route target extended community attributes satisfy the matching conditions are reflected. This provides a way to implement load balancing between RRs.

Example # In BGP-VPNv4 subaddress family view, create an RR group and configure it to automatically filter the incoming VPNv4 route update packets based on the route target extended community attribute.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] ipv4-family vpnv4
[Sysname-bgp-af-vpnv4] rr-filter 10
```

In BGP-L2VPN address family view, create an RR group and configure it to automatically filter the incoming VPNv4 route update packets based on the route target extended community attribute.

```
<Sysname> system-view
[Sysname] bgp 100
[Sysname-bgp] l2vpn-family
[Sysname-bgp-af-l2vpn] rr-filter 10
```

sham-link

Syntax **sham-link** *source-ip-address destination-ip-address* [**cost** *cost* | **dead** *dead-interval* | **hello** *hello-interval* | **retransmit** *retrans-interval* | **trans-delay** *delay* | **simple** [**cipher** | **plain**] *password1* | { **md5** | **hmac-md5** } *key-id* [**cipher** | **plain**] *password2*] *

undo sham-link *source-ip-address destination-ip-address* [**cost** | **dead** | **hello** | **retransmit** | **trans-delay** | **simple** | { **md5** | **hmac-md5** } *key-id*] *

View OSPF area view

Parameter *source-ip-address*: Source IP address for the sham link.

destination-ip-address: Destination IP address for the sham link.

cost: Cost for the sham link. It ranges from 1 to 65,535 and defaults to 1.

dead-interval: Dead Interval in seconds. It ranges from 1 to 32,768 and defaults to 40. It must be equal to the dead interval of the router on the other end of the virtual link and be at least four times the hello interval.

hello-interval: Interval at which the interface sends Hello packets. It ranges from 1 to 8,192 seconds and defaults to 10 seconds. It must be equal to the hello interval of the router on the other end of the virtual link.

retrans-interval: Interval at which the interface retransmits LSAs. It ranges from 1 to 8,192 seconds and defaults to 5 seconds.

delay: Delay interval before the interface sends an LSA. It ranges from 1 to 8,192 seconds and defaults to 1 second.

simple [**cipher** | **plain**] *password1*: Uses simple authentication. If you specify neither the **cipher** nor the **plain** keyword, the *password1* argument is a string of 1 to 8 characters. For the plain mode, the *password1* argument is a string of 1 to 8 characters. For the cipher mode, the *password1* argument can be either a string of 1 to 8 characters in plain text, or a string of 24 characters in cipher text.

md5: Uses MD5 algorithm for authentication.

hmac-md5: Uses HMAC-MD5 algorithm for authentication.

key-id: Authentication key ID of the interface, in the range 1 to 255. It must be the same as that of the peer.

cipher: Uses cipher text.

plain: Uses plain text.

password2: Password string, case sensitive. If you specify neither the **cipher** nor the **plain** keyword, it is a string of 1 to 16 characters in plain text or a string of 24 characters in cipher text. For the plain mode, it is a string of 1 to 16 characters. For the cipher mode, it can be either a string of 1 to 16 characters in plain text, or a string of 24 characters in cipher text.

Description

Use the **sham link** command to configure a sham link.

Use the **undo sham link** command with no optional keyword to remove a sham link.

Use the **undo sham link** command with optional keywords to restore the defaults of the parameters for a sham link.

If two PEs belong to the same AS and a backdoor link is present, a sham link can be established between them.

For plain text authentication, the default authentication key type is plain. For authentication using MD5 algorithm or HMAC-MD5 algorithm, the default authentication key type is cipher.

Example # Create a sham link with the source address of 1.1.1.1 and the destination address of 2.2.2.2.

```
<Sysname> system-view
[Sysname] ospf
[Sysname-ospf-1] area 0
[Sysname-ospf-1-area-0.0.0.1] sham-link 1.1.1.1 2.2.2.2
```

tnl-policy (VPN instance view)

Syntax **tnl-policy** *tunnel-policy-name*

undo tnl-policy

View VPN instance view

Parameter *tunnel-policy-name*: Name of the tunneling policy for the VPN instance, a string of 1 to 19 characters.

Description Use the **tnl-policy** command to associate the current VPN instance with a tunneling policy.

Use the **undo tnl-policy** command to remove the association.

When selecting tunnels from the VPN tunnel management module, an application can use the tunneling policy as the criterion. With no tunneling policy associated with a VPN instance, the default tunneling policy is used.

Related command: **tunnel select-seq load-balance-number**.

Example # Associate VPN instance vpn2 with tunneling policy po1.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1] tunnel select-seq lsp load-balance-number 1
[Sysname-tunnel-policy-po1] quit
[Sysname] ip vpn-instance vpn2
[Sysname-vpn-instance-vpn2] route-distinguisher 22:33
[Sysname-vpn-instance-vpn2] tnl-policy po1
```

tunnel-policy

Syntax **tunnel-policy** *tunnel-policy-name*

undo tunnel-policy *tunnel-policy-name*

View System view

Parameter *tunnel-policy-name*: Name for the tunneling policy, a string of 1 to 19 characters.

Description Use the **tunnel-policy** command to establish a tunneling policy and enter tunneling policy view.

Use the **undo tunnel-policy** command to delete a tunneling policy.

Related command: **tunnel select-seq load-balance-number**.

Example # Establish a tunneling policy named po1 and enter tunneling policy view.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1]
```

tunnel select-seq load-balance-number

Syntax **tunnel select-seq** { **cr-lsp** | **gre** | **lsp** }* **load-balance-number** *number*

undo tunnel select-seq

View Tunneling policy view

Parameter **cr-lsp**: Specifies CR-LSP tunnels.

gre: Specifies GRE tunnels.

lsp: Specifies LSP tunnels.

number: Number of tunnels for load balancing, in the range 1 to 8.

Description Use the **tunnel select-seq load-balance-number** command to configure the preference order for tunnel selection and the number of tunnels for load balancing.

Use the **undo tunnel select-seq** command to restore the default.

By default, one LSP tunnel can be used. That is, only LSP tunnels can be used and the number of tunnels for load balancing is 1.

Note that:

- Only tunnels of the types specified in the **tunnel select-seq load-balance-number** command can be used.
- A tunnel type closer to the **select-seq** keyword has a higher priority.
- The number of tunnels for load balancing refers to the number of tunnels that an application can use.

CR-LSP tunnels are preferred by the following order: CR-LSPs configured with ACLs, CR-LSPs bound with VPN, and ordinary CR-LSPs. These three types of CR-LSPs are mutually exclusive, that is, only one type of the three is selected at a time.

Example # Define a tunneling policy, specifying that only GRE tunnels can be used and the number of tunnels for load balancing be 2.

```
<Sysname> system-view
[Sysname] tunnel-policy po1
[Sysname-tunnel-policy-po1] tunnel select-seq gre load-balance-number 2
```

vpn-instance-capability simple

Syntax **vpn-instance-capability simple**

undo vpn-instance-capability

View OSPF multi-instance view

Parameter None

Description Use the **vpn-instance-capability simple** command to enable multi-VPN-instance CE.

Use the **undo vpn-instance-capability** command to disable the function.

By default, the function is disabled.

Example # Enable multi-VPN-instance CE.

```
<Sysname> system-view
[Sysname] ospf 100 vpn-instance vpna
[Sysname-ospf-100] vpn-instance-capability simple
```

vpn-target (VPN instance view)

Syntax **vpn-target** *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**]

undo vpn-target { **all** | { *vpn-target*&<1-8> [**both** | **export-extcommunity** | **import-extcommunity**] } }

View VPN instance view

Parameter *vpn-target*&<1-8>: Adds the VPN target extended community attribute to the import or export VPN target extended community list and specify the VPN target in the format nn:nn or IP-address:nn. &<1-8> means that you can specify this argument for up to 8 times.

A VPN target attribute can be of 3 to 21 characters and in either of these two formats:

- 16-bit AS number: 32-bit user-defined number. For example, 101:3.
- 32-bit IP address: 16-bit user-defined number. For example, 192.168.122.15:1.

both: Specifies both the export routing information to the destination VPN extended community and the import routing information from the destination VPN extended community. This is the default.

export-extcommunity: Specifies the export routing information to the destination VPN extended community.

import-extcommunity: Specifies the import routing information from the destination VPN extended community.

all: Specifies all export routing information to the destination VPN extended community and import routing information from the destination VPN extended community.

Description Use the **vpn-target** command to associate the current VPN instance with one or more VPN targets.

Use the **undo vpn-target** command to remove the association of the current VPN instance with VPN targets.

VPN target has no default. You must configure it when creating a VPN instance.

Example # Associate the current VPN instance with VPN targets.

```
<Sysname> system-view
[Sysname] ip vpn-instance vpn1
[Sysname-vpn-instance-vpn1] vpn-target 3:3 export-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 4:4 import-extcommunity
[Sysname-vpn-instance-vpn1] vpn-target 5:5 both
```

99 VAM SERVER CONFIGURATION COMMANDS

authentication-algorithm

Syntax **authentication-algorithm** { **none** | { **md5** | **sha-1** }* }

undo authentication-algorithm

View VPN domain view

Parameter **none**: Specifies not to authenticate protocol packets.

md5: Specifies to adopt MD5 (message digest 5) authentication.

sha-1: Specifies to adopt SHA-1 (secure hash algorithm 1) algorithm.

Description Use the **authentication-algorithm** command to set the authentication algorithm and its corresponding priority for protocol packets.

Use the **undo authentication-algorithm** command to restore the default.

By default, the authentication algorithm is SHA-1.

Note that:

- Priorities of authentication algorithms are decided by their configuration order.
- Based on its authentication algorithm configuration, a VAM server negotiates with a client to determine the authentication algorithm to be used between them.

Related command: **vam server vpn**, **authentication-method**.

Example # Set to adopt MD5 authentication algorithm in VPN domain 1.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] authentication-algorithm md5
```

authentication-method

Syntax **authentication-method** { **none** | [**chap** | **pap**] [**domain** *name-string*] }

undo authentication-method

View VPN domain view

Parameter **none**: Specifies not to authenticate clients.

pap: Specifies to adopt PAP (password authentication protocol) authentication.

chap: Specifies to adopt CHAP (challenge authentication protocol) authentication.

domain *name-string*: Specifies the ISP domain for authentication by its name, which is a case-insensitive string of 1 to 24 characters.

Description Use the **authentication-method** command to configure the mode for the VAM server to authenticate clients.

Use the **undo authentication-method** command to restore the default.

By default, CHAP authentication is adopted and the ISP domain is the default domain of the system that you configure.

Related command: **vam server vpn**, **authentication-algorithm**.

Example # Set the VAM server to authenticate clients using CHAP.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] authentication-method chap
```

display vam server address-map

Syntax **display vam server address-map** { **all** | **vpn** *vpn-name* [**private-ip** *private-ip*] }

View Any view

Parameter **all**: Displays address mapping information about all registered VAM clients on the VAM server.

vpn *vpn-name*: Displays address mapping information about all registered VAM clients in the VPN domain. The *vpn-name* argument indicates the VPN domain name, a case-insensitive string of 1 to 15 characters.

private-ip *private-ip*: Displays address mapping information about the VAM client with the specified private IP address. The *private-ip* argument indicates the private IP address of the VAM client.

Description Use the **display vam server address-map** command to display address mapping information about the registered clients on the server.

Example # Display mapping information of the VAM clients in VPN domain 1.

```
<Sysname> display vam server address-map vpn 1
VPN name:    1
```

```
Total address-map number:    2
Private-ip     Public-ip        Type        Holding time
10.0.0.1       222.222.222.1    Hub         0H 3M 34S
10.0.0.3       222.222.222.3    Spoke       0H 4M 21S
```

Display mapping information of the VAM clients in all VPN domains.

```
<Sysname> display vam server address-map all
VPN:    1            Total address-map number:    2
Private-ip     Public-ip        Type        Holding time
10.0.0.1       222.222.222.1    Hub         0H 3M 34S
10.0.0.3       222.222.222.3    Spoke       0H 4M 21S

VPN:    2            Total address-map number:    1
Private-ip     Public-ip        Type        Holding time
20.0.0.1       222.222.32.1     Hub         0H 3M 34S
```

Display mapping information of the VAM client with a private IP address of 10.0.01 in VPN domain 1.

```
<Sysname> display vam server address-map vpn 1 private-ip 10.0.0.1
VPN:    1
Private-ip     Public-ip        Type        Holding time
10.0.0.1       222.222.222.1    Hub         0H 3M 34S
```

Table 462 Description on the fields of display vam server address-map

Field	Description
VPN	Name of the VPN
Total address-map number	Total number of address mappings
Private-ip	Private address that the VAM client registers with the VAM server
Public-ip	Public address that the VAM client registers with the VAM server
Type	Type of the VAM client, Hub or Spoke
Holding time	Time that elapses since the VAM client registers with the server successfully, in the format xxH xxM xxS (xxhour xxminute xxsecond).

display vam server statistic

Syntax **display vam server statistic** { **all** | **vpn** *vpn-name* }

View Any view

Parameter

- **all**: Displays the statistics of all clients registered on the VAM server.

vpn *vpn-name*: Displays the statistics of the VAM server in the specified VPN domain. The *vpn-name* argument indicates the VPN domain name, a case-insensitive string of 1 to 15 characters.

Description Use the **display vam server statistic** command to display statistics of the VAM server.

Example # Display statistics of the VAM server.

```
<Sysname> display vam server statistic all
VPN number:                   2
Total spoke number:           121
Total hub number:             3

VPN name:    1
  Service:    enable
  Holding time: 0h 1m 47s
  Registered spoke number:    98
  Registered hub number:      2
  Address resolution times:      11
  Succeeded resolution times:    10
  Failed resolution times:    1

VPN name:    9
  Service:    enable
  Holding time: 0h 33m 53s
  Registered spoke number:    23
  Registered hub number:        1
  Address resolution times:     150
  Succeeded resolution times:    148
  Failed resolution times:    2
```

Display statistics of VPN domain 1 on the VAM server.

```
<Sysname> display vam server statistic vpn 1
VPN name:    1
  Service:    enable
  Holding time: 0h 0m 5s
  Registered spoke number:    98
  Registered hub number:    2
  Address resolution times:           11
  Succeeded resolution times:         10
  Failed resolution times:             1
```

Table 463 Description on the fields of the display vam server statistic command

Field	Description
VPN number	Number of VPN domains on the VAM server
Total spoke number	Number of Spokes on the VAM server
Total hub number	Number of Hubs on the VAM server
VPN name	Name of the VPN
Service	Whether VAM service is enabled for the VPN domain
Holding time	Time that elapses since the VAM service is enabled
Registered spoke number	Number of registered Spokes in the VPN domain
Registered hub number	Number of registered Hubs in the VPN domain
Address resolution times	Number of address resolution times in the VPN domain
Succeeded resolution times	Number of successful address resolution times in the VPN domain
Failed resolution times	Number of unsuccessful address resolution times in the VPN domain

encryption-algorithm

Syntax **encryption-algorithm** { **none** | { **aes-128** | **des** | **3des** }* }

undo encryption-algorithm

View VPN domain view

Parameter **none**: Specifies not to encrypt control packets.

aes-128: Specifies to adopt AES encryption algorithm, with the key length being 128 bits.

des: Specifies to adopt DES encryption algorithm.

3des: Specifies to adopt 3DES encryption algorithm.

Description Use the **encryption-algorithm** command to configure the encryption and its corresponding priority for protocol packets.

Use the **undo encryption-algorithm** command to restore the default.

By default, AES-128, 3DES and DES are adopted, with their priorities from the highest to the lowest being AES-128, 3DES, and DES.

Note that:

- Priorities of encryption algorithms are decided by their configuration order.
- Based on its encryption algorithm configuration, a VAM server negotiates with a client to determine the encryption algorithm to be used between them.

Related command: **vam server vpn**.

Example # Specifies to adopt AES-128 and 3DES encryption algorithms in VPN domain 1, with the priority of AES-128 higher than that of 3DES.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] encryption-algorithm aes-128 3des
```

hub private-ip

Syntax **hub private-ip** *private-ip-address* [**public-ip** *public-ip-address*]

undo hub private-ip *private-ip-address*

View VPN domain view

Parameter *private-ip-address*: Private IP address of Hub.

public-ip-address: Public IP address of Hub.

Description Use the **hub private-ip** command to specify the IP address of Hub.

Use the **undo hub private-ip** command to remove the IP address of the specified Hub.

By default, no Hub IP address is configured.

Note that:

- You can specify only the private IP address of Hub. When Hub is added to a VPN domain, the VAM server can obtain the mapping information between the registered public and private addresses of the Hub.
- Currently, up to two Hub addresses can be configured on the VAM server.

Related command: **vam server vpn**.

Example # Specifies in VPN 1 the public and private IP addresses of Hub as 123.0.0.1 and 10.1.1.1 respectively.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] hub private-ip 10.1.1.1 public-ip 123.0.0.1
```

keepalive interval

Syntax **keepalive interval** *time-interval*

undo keepalive interval

View VPN domain view

Parameter *time-interval*: Interval for sending keepalive message from VAM client. It is in the range 5 to 60 seconds.

Description Use the **keepalive interval** command to configure the interval for sending keepalive messages from VAM client to VAM server.

Use the **undo keepalive interval** command to restore to the default value.

By default, the interval for sending keepalive message from VAM client is 10 seconds.

Note that the VAM server sends this setting in a registration response to its clients. All clients in a VPN have the same keepalive settings, but if you change the keepalive settings of the server, the new settings are sent to only clients that register later; all clients registering before use the old settings.

Related command: **vam server vpn**, **keepalive retry**

Example # Configure the interval for sending keepalive messages from VAM client to VAM server to 30 seconds.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] keepalive interval 30
```

keepalive retry

Syntax **keepalive retry** *retry-times*

undo keepalive retry

View VPN domain view

Parameter *retry-times*: Maximum number of attempts of sending keepalive message from VAM client. It is in the range 1 to 6.

Description Use the **keepalive retry** command to configure the maximum number of attempts of sending keepalive message from VAM client to VAM server. If the maximum number of attempts is reached but no response is received by a VAM client, the VAM client regards that the connection is broken.

Use the **undo keepalive retry** command to restore to the default value.

By default, the maximum number of attempts of sending keepalive message from VAM client is 3.

Note that the VAM server sends this setting in a registration response to its clients. All clients in a VPN have the same keepalive settings, but if you change the keepalive settings of the server, the new settings are sent to only clients that register later; all clients registering before use the old settings.

Related command: **vam server vpn**, **keepalive interval**

Example # Configure the maximum number of attempts of sending keepalive message from VAM client to 5.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] keepalive retry 5
```

pre-shared-key (VPN domain view)

Syntax **pre-shared-key** { **cipher** | **simple** } *key-string*

undo pre-shared-key

View VPN domain view

Parameter **cipher**: Specifies to display pre-shared key in cipher text.

simple: Specifies to display pre-shared key in plain text.

key-string: Pre-shared key to be specified, a case-sensitive string containing 1 to 31 characters.

Description Use the **pre-shared-key** command to configure a pre-shared key for VAM server. The pre-shared key is used as a public initial key for every encryption algorithm that encrypts VAM control packets.

Use the **undo pre-shared-key** command to remove a pre-shared key.

By default, no pre-shared key is configured.

Related command: **vam server vpn**, **pre-shared-key (VAM client view)**, **authentication-algorithm**, **encryption-algorithm**

Example # Configure the pre-shared key for VAM server to 123, which is displayed in plain text.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] pre-shared-key simple 123
```

server enable

Syntax **server enable**

undo server enable

View VPN domain view

Parameter None

Description Use the **server enable** command to enable the VAM server function of a specific VPN domain.

Use the **undo server enable** command to disable the VAM server function of a specific VPN domain.

By default, VAM server function is disabled.

Related command: **vam server vpn**, **vam server enable**

Example # Enable the VAM server function of VPN domain 1.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1] server enable
```

vam server enable

Syntax **vam server enable** { **all** | **vpn** *vpn-name* }

undo vam server enable { **all** | **vpn** *vpn-name* }

View System view

Parameter **all**: Specifies all VPN domains whose VAM server function is to be enabled or disabled.

vpn *vpn-name*: Specifies an existing VPN domain. The *vpn-name* argument indicates the VPN domain name and is a case-insensitive string of 1 to 15 characters. Valid characters are A to Z, a to z, 0 to 9, and ".".

Description Use **vam server enable** command to enable the VAM server function of all VPN domains or a specific VPN domain.

Use the **undo vam server enable** command to disable the VAM server function of all VPN domains or a specific VPN domain.

By default, VAM server function is disabled.

Related command: **vam server vpn**, **server enable**

Example # Enable the VAM server function of all VPN domains.

```
<Sysname> system-view
[Sysname] vam server enable all
```

vam server ip-address

Syntax **vam server ip-address** *ip-address* [**port** *port-number*]

undo vam server ip-address

View System view

Parameter *ip-address*: Listening IP address to be assigned to a VAM server.

port-number: Listening UDP port number to be configured to a VAM server. By default, it is 40000.

Description Use the **vam server ip-address** command to configure the listening IP address and UDP port number for VAM server.

Use the **undo vam server ip-address** command to remove the configured listening IP address and UDP port number.

By default, listening IP address and UDP port number are not configured.

Note that the VAM server only accepts the connections of all VPN domains through the configured UDP port.

Related command: **vam server vpn**

Example # Configure the listening IP address to 10.1.1.1 and UDP port number to 40000 for a VAM server.

```
<Sysname> system-view
[Sysname] vam server ip-address 10.1.1.1 port 40000
```

vam server vpn

Syntax **vam server vpn** *vpn-name*

undo vam server vpn *vpn-name*

View System view

Parameter *vpn-name*: VPN domain name. It is a case-insensitive string containing 1 to 15 characters, which can be A to Z, a to z, 0 to 9, hyphen sign, and dot sign.

Description Use the **vam server vpn** command to create a VPN domain and enter its view. If a VPN domain with the same name already exists, executing this command will enter the VPN domain view.

Use the **undo vam server vpn** command to remove a specified VPN domain.

By default, there is no VPN domain.

Example # Create VPN domain 1 and enter its view.

```
<Sysname> system-view
[Sysname] vam server vpn 1
[Sysname-vam-server-vpn-1]
```

100

VAM CLIENT CONFIGURATION COMMANDS

client enable

Syntax **client enable**

undo client enable

View VAM client view

Parameter None

Description Use the **client enable** command to enable the VAM client function.

Use the **undo client enable** command to restore the default.

By default, the VAM client function is disabled.

Related command: **vam client name**, and **vam client enable**.

Example # Enable the VAM client function on client named spoke.

```
<Sysname> system-view
[Sysname] vam client name spoke
[Sysname-vam-client-name-spoke] client enable
```

display vam client

Syntax **display vam client** { **address-map** | **fsm** } [*client-name*]

View Any view

Parameter **address-map**: Refers to the mapping information between public and private network addresses of the VAM client.

fsm: Refers to the status information of the VAM client.

client-name: VAM client name, a case-insensitive string of 1 to 31 characters.

Description Use the **display vam client** command to display registration information of the VAM client.

On a Spoke, the command displays the address mapping information of the other Spokes and the Hubs that is received from the VAM server. On a Hub, the command displays the address mapping information of the other Hubs that is received from the VAM server.

Note that:

- If *client-name* is specified, the registration information of a specific VAM client is displayed.
- If *client-name* is not specified, the registration information of all VAM clients is displayed.
- As for the arguments not specified, or the information not obtained dynamically, the corresponding information will not be displayed.

Example # Display the status information of VAM client abc.

```
<Sysname> display vam client fsm abc
Client name: hub
 VPN name:  1
 Interface: Tunnel0
 Resend interval(seconds): 5
 Client type: Hub
 Username: user1

 Primary server:   28.1.1.23
   Current state:  ONLINE
   Holding time:   9h 20m 30s
   Encryption-algorithm:     AES-128
   Authentication-algorithm: SHA1
Secondary server: 28.1.1.33
   Current state:  OFFLINE
   Holding time:   1h 24m 1s
   Encryption-algorithm:     AES-128
   Authentication-algorithm: SHA1
```

Table 464 Description on the fields of the display vam client fsm command

Field	Description
Client name	Name of the VAM client
VPN name	Name of the VPN domain where the VAM client resides
Interface	DVPN tunnel interface of the VAM client
Resend interval(seconds)	Protocol message retransmission interval of the VAM client
Client type	VAM client type, Hub or Spoke
Username	Username of the VAM client

Table 464 Description on the fields of the display vam client fsm command

Field	Description
Primary server	Public IP address of the primary VAM server
Current state	Current authentication status of the VAM client
Primary server	IP address of the primary VAM server
Holding time	Period of time that the VAM client is up
Encryption-algorithm	Negotiated encryption algorithm
Authentication-algorithm	Negotiated authentication algorithm
Secondary server	Public IP address of the secondary VAM server

Display the cached address mapping information on the VAM client.

```
<Sysname> display vam client address-map abc
Client name:    abc
VPN name:    1
Total address-map number:    2
Private-ip     Public-ip        Type   Remaining-time(s)
10.0.0.1       222.222.222.1    Hub    --
10.0.0.3       222.222.222.3    Spoke  32
```

Table 465 Description on the fields of display vam server address-map

Field	Description
Client name	Name of the VAM client
VPN name	Name of the VPN domain where the VAM client resides
Total address-map number	Number of VAM client private-public address mappings in the VPN domain
Private-ip	Private IP address
Public-ip	Public IP address corresponding to the private IP address
Type	Type of the VAM client
Remaining-time(s)	Remaining time before the mapping entry gets aged out

pre-shared-key (VAM client view)

Syntax **pre-shared-key** { **cipher** | **simple** } *key-string*

undo pre-shared-key

View VAM client view

Parameter **cipher**: Specifies a pre-shared key in cipher text.

simple: Specifies a pre-shared key in plain text.

key-string: Pre-share key, in the range 1 to 31 case sensitive characters.

Description Use the **pre-shared-key** command to configure a pre-shared key for the VAM client. The pre-shared key is an initial public key used for the establishment of a secured tunnel for the VAM client and VAM server to exchange protocol packets.

Use the **undo pre-shared-key** command to delete the configured pre-shared key. That is, no encryption or authentication is performed on protocol packets.

No pre-shared key is configured by default.

Note that you should configure the same pre-shared keys for all the devices on the same VPN. The VAM server generates keys based on the configured pre-shared key to protect initialization packets.

Related command: **vam client name**, and **pre-shared-key (VPN domain view)**.

Example # Configure the pre-shared key for the VAM client to 123 in plain text.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] pre-shared-key simple 123
```

resend interval

Syntax **resend interval** *time-interval*

undo resend interval

View VAM client view

Parameter *time-interval*: Protocol packet retransmission interval, in the range 3 to 30 seconds.

Description Use the **resend interval** command to configure the interval for the VAM client to resend VAM protocol packets.

Use the **undo resend interval** command to restore the default.

By default, the retransmission interval is 5 seconds.

After sending protocol packets to the VAM server, the VAM client will resend the packets if no response is received from the server within the specified interval. The protocol packets include: initialization request packets, initialization finished packets, registration request packets, authentication request packets, address resolution packets, and stop-accounting packets.

Related command: **vam client name**.

Example # Configure the interval for the VAM client to resend VAM protocol packets to 20 seconds.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] resend interval 20
```

server primary ip-address

Syntax **server primary ip-address** *ip-address* [**port** *port-number*]

undo server primary

View VAM client view.

Parameter *ip-address*: Public IP address of the primary VAM server. DNS is not supported currently.

port-number: Port number of the primary VAM server, in the range 1025 to 65535. It defaults to 40959.

Description Use the **server primary ip-address** command to specify public IP address and UDP port number for the primary VAM server.

Use the **undo server primary** command to restore the default.

By default, no public IP address or UDP port number is specified for the primary VAM server.

Related command: **vam client name**, and **server secondary ip-address**.

Example # Specify public IP address 1.1.1.1 and port number 40000 for the primary VAM server.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] server primary ip-address 1.1.1.1 port 40000
```

server secondary ip-address

Syntax **server secondary ip-address** *ip-address* [**port** *port-number*]

undo server secondary [**ip-address** *ip-address*]

View VAM client view

Parameter *ip-address*: Public IP address of the secondary VAM server. DNS is not supported currently.

port-number: Port number of the secondary VAM server, in the range 1025 to 65535. It defaults to 40000.

Description Use the **server secondary ip-address** command to configure public IP address and UDP port number for the secondary VAM server.

Use the **undo server secondary ip-address** command to remove the specified or all public IP address(es) and port number(s).

By default, no public IP address or UDP port number is specified for the secondary VAM server.

Related command: **vam client name**, and **server primary ip-address**.

Example # Specify public IP address 1.1.1.2 and port number 50000 for the secondary VAM server.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] server secondary ip-address 1.1.1.2 port 50000
```

user

Syntax **user** *username* **password** { **cipher** | **simple** } *string*

undo user

View VAM client view

Parameter *Username:* Username of a VAM client, a string of 1 to 55 characters, excluding special characters /, :, *, ?, <, >, @, |, , and ".

cipher: Displays a password in the cipher text mode.

simple: Displays a password in the plain text mode.

String: Password of a VAM client, a case sensitive string of 1 to 63 characters.

Description Use the **use**r command to configure a local username and password.

Use the **undo user** command to remove the configuration.

By default, no local username or password is configured.

Note that only one local username can be configured in VAM client view.

Related command: **vam client name**.

Example # Set the local username and password both to user.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] user user password simple user
```

vam client enable

Syntax **vam client enable** { **all** | **name** *client-name* }

undo vam client enable { **all** | **name** *client-name* }

View System view

Parameter **all**: Specifies all configured VAM clients.

name *client-name*: Specifies an existing VAM client. The *client-name* argument indicates the name of the VAM client and is a case-insensitive string of 1 to 31 characters. Valid characters are A to Z, a to z, 0 to 9, and ".".

Description Use the **vam client enable** command to enable all VAM clients or a specified VAM client.

Use the **undo vam client enable** command to disable all VAM clients or a specified VAM client.

By default, all VAM clients are disabled.

Related command: **vam client name** and **client enable**.

Example # Enable the VAM client named spoke.

```
<Sysname> system-view
[Sysname] vam client enable name spoke
```

vam client name

Syntax **vam client name** *client-name*

undo vam client name *client-name*

View System view

Parameter *client-name*: Name of a VAM client, a string of 1 to 31 case-insensitive characters. Valid characters are A through Z, a through z, 0 through 9, hyphen (-), and dot (.).

Description Use the **vam client** command to create a VAM client and enter VAM client view, or enter VAM client view directly if the VAM client already exists.

Use the **undo vam client** command to delete the specified VAM client.

By default, no VAM client is configured.

Note that you are unable to directly delete a VAM client that is already applied on an interface.

Example # Create a VAM client named abc.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc]
```

vpn

Syntax **vpn** *vpn-name*

undo vpn

View VAM client view

Parameter *vpn-name*: Name of the VPN that a VAM client belongs to, a case-insensitive string of 1 to 15 characters A through Z, a through z, 0 through 9, hyphen (-), and dot (.).

Description Use the **vpn** command to specify the VPN that a VAM client belongs to.

Use the **undo vpn** command to remove the configuration.

By default, a VAM client does not belong to any VPN.

Related command: **vam client name**.

Example # Specify the VAM client "abc" to belong to VPN 100.

```
<Sysname> system-view
[Sysname] vam client name abc
[Sysname-vam-client-name-abc] vpn 100
```

101

IPSEC PROFILE CONFIGURATION COMMANDS

display ipsec profile

Syntax **display ipsec profile** [**name** *profile-name*]

View Anyview

Parameter *profile-name*: Name of the IPSec profile, a case-insensitive string of 1 to 15 characters.

Description Use the **display ipsec profile** command to display information about a specified or all IPSec profiles.

Note that if the *profile-name* keyword is not specified, this command will display information about all IPSec profiles.

Related command: **ipsec profile (system view)**.

Example # Display information about all IPSec profiles.

```
<Sysname> display ipsec profile
=========================================
IPsec profile: "abc"
Using interface: {Tunnel0}
=========================================

  -----------------------------------
  IPsec profile name: "abc"
  mode: dvpn
  -----------------------------------
    tunnel local address: 162.105.10.1
    tunnel remote address: dynamic
    perfect forward secrecy: None
    proposal name: prop1
    ipsec sa local duration(time based): 3600 seconds
    ipsec sa local duration(traffic based): 1843200 kilobytes
```

```
inbound ESP setting:
      ESP spi: 23456 (0x5ba0)
      ESP string-key:
      ESP encryption hex key:
                  1234567890abcdef1234567890abcdef1234567812345678
      ESP authentication hex key: 1234567890abcdef1234567890abcdef
outbound ESP setting:
      ESP spi: 65432 (0xff98)
      ESP string-key:
      ESP encryption hex key:
                  11223344556677889900aabbccddeeff1234567812345678
      ESP authentication hex key: 11223344556677889900aabbccddeeffIPsec
```

Table 466 Description on the fields of the display ipsec profile command

Field	Description
IPsec profile name	Name of the IPSec profile
mode	Tunneling mode used by the IPSec profile
tunnel local address	Local address of the tunnel
tunnel remote address	Remote address of the tunnel
perfect forward secrecy	PFS feature that is configured
proposal name	IPSec proposal referenced by the IPSec profile
ipsec sa local duration(time based)	Local time-based SA lifetime
ipsec sa local duration(traffic based)	Local traffic-based SA lifetime
inbound ESP setting	ESP settings in the inbound direction
outbound ESP setting	ESP settings in the outbound direction
ESP spi	Security parameter index (SPI) of the SA using ESP
ESP string-key	Key of the SA using ESP
ESP encryption hex key	Encryption key of the SA using ESP, in hexadecimal.
ESP authentication hex key	Authentication key of the SA using ESP, in hexadecimal.

ipsec profile (system view)

Syntax **ipsec profile** *profile-name*

undo ipsec profile *profile-name*

View System view

Parameter *profile-name*: Name of the IPSec profile, a case-insensitive string of 1 to 15 characters.

Description Use the **ipsec profile** command to create an IPSec profile and enter its view.

Use the **undo ipsec profile** command to remove a specified IPSec profile.

By Default, no IPSec profile exists.

Note that:

An IPSec profile sets up an SA through IKE negotiation.

You must specify the ESP protocol as a security protocol for IPSec proposals in the IPSec profile.

An IPSec profile simplifies the configuration of an IPSec policy. Some parameters are set to the default values.

Due to the dynamics of DVPN addresses, the setting by the **remote-address** keyword for the IKE peer that an IPSec profile references does not take effect on the initiator.

Example # Create an IPSec profile named dvpnprofile and enter its view.

```
<Sysname> system-view
[Sysname] ipsec profile dvpnprofile
[Sysname-ipsec-profile-dvpnprofile]
```

102

DVPN TUNNEL CONFIGURATION COMMANDS

display dvpn session

Syntax **display dvpn session** { **all** | **interface** *interface-type interface-number* [**private-ip** *ip-address*] }

View Any view

Parameter **All**: Displays information about all Spoke-Spoke and Spoke-Hub sessions associated with the VAM client.

interface *interface-type interface-number*: Displays information about DVPN sessions associated with the interface specified by *interface-type* and *interface-number*. The interface must be of the type of tunnel.

private-ip *ip-address*: Specifies the private IP address of the peer VAM client.

Description Use the **display dvpn session** to display information about the DVPN session list.

Example # Display information about DVPN sessions associated with interface Tunnel0.

```
<Sysname> display dvpn session interface tunnel 0
Interface: Tunnel0  Total number: 2

  Private IP:     10.0.0.21
  Public IP:      28.1.1.21
  Tunnel type:    Hub-Spoke
  State:  SUCCESS
  Holding time: 0h 15m 33s
  Input:  277 packets,  66 data packets,  211 control packets
           58 multicasts,  0 errors
  Output: 279 packets,  103 data packets,  176 control packets
           93 multicasts,  0 errors
```

```
Private IP:     10.0.0.22
Public IP:      28.1.1.22
Tunnel type:    Hub-Spoke
State:  SUCCESS
Holding time: 0h 44m 9s
Input:  279 packets,  100 data packets,  179 control packets
         91 multicasts,  0 errors
Output: 273 packets,  99 data packets,  174 control packets
         91 multicasts,  0 errors
```

Table 467 Description on the fields of the display dvpn session command

Field	Description
Interface	DVPN tunnel interface
Total number	Total number of DVPN tunnels established on the tunnel interface
Private IP	Private address of the DVPN tunnel peer
Public IP	Public address of the DVPN tunnel peer
Tunnel type	Type of the DVPN tunnel
State	Status of the DVPN tunnel, which can be SUCCESS, ESTABLISH, or DUMB. ■ SUCCESS: Indicates that the tunnel is already established. ■ ESTABLISH: Indicates that the tunnel is being established. ■ DUMB: Indicates that the tunnel failed to be established and is now quiet.
Holding time	Length of time that the tunnel is in the current state
Input	Statistics about inbound packets, including the counts of all packets, data packets, control packets, multicast packets, and erroneous packets.
Output	Statistics about outbound packets, including the counts of all packets, data packets, control packets, multicast packets, and erroneous packets.

dvpn session dumb-time

Syntax **dvpn session dumb-time** *time-interval*

undo dvpn session dumb-time

View Tunnel interface view

Parameter *time-interval*: Quiet period after the DVPN tunneling fails in seconds, in the range 10 to 600.

Description Use the **dvpn session dumb-time** command to configure the quiet period when the attempts for DVPN tunneling reach the maximum value. After the quiet period elapsed, the device initiates a new DVPN tunneling.

Use the **undo dvpn session dumb-time** command to restore the default.

By default, the quiet period is 120 seconds.

Note that the VAM client triggers the quiet timer only when the attempts for tunneling the Hub reach the maximum value.

Related command: **interface tunnel** on page 884 and **tunnel-protocol** on page 887.

Example # Set the quiet period to 100 seconds for VAM client abc when the attempts for tunneling the Hub reach the maximum value.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] dvpn session dumb-time 100
```

dvpn session idle-time

Syntax **dvpn session idle-time** *time-interval*

undo dvpn session idle-time

View Tunnel interface view

Parameter *time-interval*: Idle timeout for a Spoke-Spoke type DVPN tunnel in seconds, in the range 60 to 1,800.

Description Use the **dvpn session idle-time** command to configure the idle timeout of a Spoke-Spoke type DVPN tunnel, that is, the tunnel will be removed automatically if no data flows are transferred through a Spoke-Spoke type DVPN tunnel during the idle timeout time.

Use the **undo dvpn session idle-time** command to restore the default.

By default, the idle timeout for a Spoke-Spoke type DVPN tunnel is 300 seconds.

Note that all VAM clients in a VPN domain must have the same configuration.

Related command: **interface tunnel** on page 884 and **tunnel-protocol** on page 887.

Example # Set the idle timeout for a Spoke-Spoke type DVPN tunnel to 600 seconds.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-tunnel0] dvpn session idle-time 600
```

ipsec profile (tunnel interface view)

Syntax **ipsec profile** *ipsec-profile-name*&<1-6>

undo ipsec profile [*ipsec-profile-name*&<1-6>]

View Tunnel interface view

Parameter *ipsec-profile-name*&<1-6>: Name of the IPSec profile used for protecting data packets and control packets passing through a DVPN tunnel, a case-insensitive

string of 1 to 15 characters. &<1-6> means that you can specify the argument for up to 6 times.

Description Use the **ipsec profile** command to configure to reference an IPSec profile on a DVPN tunnel interface.

Use the **undo ipsec profile** command to cancel the reference of an IPSec profile on a DVPN tunnel interface.

By default, no IPSec profile exists. That is, DVPN tunnels are not protected.

Note that:

IPSec profiles are applicable only for the interfaces of DVPN-type tunnels.

A DVPN tunnel interface can reference only one IPSec profile.

You need cancel the currently referenced IPSec profile on a DVPN tunnel interface before referencing a new one.

Related command: **ipsec profile (system view)** and **interface tunnel** on page 884.

Example # Specify to reference IPSec profile dvpnprofile on DVPN tunnel interface Tunnel0 to protect the DVPN tunnel.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] tunnel-protocol dvpn udp
[Sysname-Tunnel0] ipsec profile dvpnprofile
```

keepalive

Syntax **keepalive** [*seconds* [*times*]]

undo keepalive

View Tunnel interface view

Parameter *seconds*: Interval in seconds for transmitting keepalive packets, in the range 1 to 32,767. The default value is 10.

times: Maximum number of attempts for transmitting a keepalive packet, in the range 1 to 255. The default value is 3.

Description Use the **keepalive** command to set the keepalive interval and the maximum number of attempts for transmitting a keepalive packet.

When the tunneling mode is DVPN, use the **undo keepalive** command to restore the default.

The command does not allow the Keepalive timer to be triggered immediately until DVPN sessions are set up successfully.

Related command: **interface tunnel** on page 884.

Example # Set the DVPN keepalive interval to 20 seconds and the maximum number of attempts for transmitting a keepalive packet to 5.

```
<Sysname> system-view
[Sysname] interface Tunnel 0
[Sysname-Tunnel0] keepalive 20 5
```

reset dvpn session

Syntax **reset dvpn session** { **all** | **interface** *interface-type interface-number* [**private-ip** *ip-address*] }

View User view

Parameter **all**: Specifies all Spoke-Spoke and Spoke-Hub tunnels connected with the VAM client.

interface *interface-type interface-number*: Specifies the DVPN tunnels on the interface. The *interface-type* argument can only be tunnel.

private-ip *ip-address*: Specifies the private IP address of the peer client.

Description Use the **reset dvpn session** command to remove DVPN tunnels connected with the current client.

Example # Remove the Spoke-Spoke tunnel on interface Tunnel0 whose peer private address is 169.254.0.1.

```
<Sysname> reset dvpn session interface tunnel 0 private-ip 169.254.0.1
```

tunnel-protocol dvpn udp

Syntax **tunnel-protocol dvpn udp**

undo tunnel-protocol

View Tunnel interface view

Parameter None

Description Use the **tunnel-protocol dvpn udp** command to configure the DVPN tunnel mode.

Use the **undo tunnel-protocol** command to restore the default.

The default mode is GRE.

Related command: **interface tunnel** on page 884.

Example # Configure the DVPN tunnel mode.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] tunnel-protocol dvpn udp
```

vam client

Syntax **vam client** *client-name*

undo vam client

View Tunnel interface view

Parameter *client-name*: Name of the VAM client, a case-insensitive string of 1 to 31 characters.

Description Use the **vam client** command to specify the VAM client to be referenced on a DVPN tunnel interface.

Use the **undo vam client** command to remove the VAM client.

By default, a DVPN tunnel interface references no VAM client.

Note that a DVPN tunnel interface can reference only one VAM client.

Related command: **interface tunnel** on page 884 and **tunnel-protocol** on page 887.

Example # Configure DVPN tunnel interface Tunnel0 to reference VAM client abc.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] vam client abc
```

103 GRE CONFIGURATION COMMANDS

destination

Syntax **destination** { *ip-address* | *ipv6-address* }

undo destination

View Tunnel interface view

Parameter *ip-address*: Destination IPv4 address for a tunnel interface.

Ipv6-address: Destination IPv6 address for a tunnel interface.

Description Use the **destination** command to specify the destination address for a tunnel interface.

Use the **undo destination** command to remove the configuration.

By default, no destination address is configured for a tunnel interface.

Note that:

- The destination address of a tunnel interface is the address of the peer interface receiving packets. It is usually set to the source address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related command: **interface tunnel**and **source**.

Example # Set Serial 2/0 (193.101.1.1) of Sysname1 and Serial 2/0 (192.100.1.1) of Sysname2 as the source/destination interface and destination/source interface of the interfaces of the tunnel between the two devices, respectively.

```
<Sysname1> system-view
[Sysname1] interface tunnel 0
[Sysname1-Tunnel0] source 193.101.1.1
[Sysname1-Tunnel0] destination 192.100.1.1
<Sysname2> system-view
[Sysname2] interface tunnel 1
[Sysname2-Tunnel1] source 192.100.1.1
[Sysname2-Tunnel1] destination 193.101.1.1
```

display interface tunnel

Syntax **display interface tunnel** [*number*]

View Any view

Parameter *number*: Tunnel interface number.

Description Use the **display interface tunnel** command to display information about a specified or all tunnel interfaces.

If the *number* argument is not specified, the command displays information about all tunnel interfaces.

Related command: **source**, **destination**, **gre key**, **gre checksum**, and **tunnel-protocol** on page 887.

Example # Display information about interface Tunnel0.

```
<Sysname> display interface tunnel 0
Tunnel0 current state: UP
Line protocol current state: UP
Description: Tunnel0 Interface
The Maximum Transmit Unit is 64000
Internet Address is 10.1.2.1/24 Primary
Encapsulation is TUNNEL, aggregation ID not set
Tunnel source 192.13.2.1, destination 192.13.2.2
Tunnel keepalive disable
Tunnel protocol/transport GRE/IP
    GRE key value is 123
    Checksumming of GRE packets enabled
    Last 300 seconds input:  0 bytes/sec, 0 packets/sec
    Last 300 seconds output:  0 bytes/sec, 0 packets/sec
    361 packets input,  9953388 bytes
    0 input error
    361 packets output,  30324 bytes
    0 output error
```

Table 468 Description on the fields of the display interface tunnel command

Field	Description
Tunnel0 current state	Status of the physical layer of the tunnel interface, UP or DOWN
Line protocol current state	Status of the link layer of the tunnel interface, UP or DOWN
Description	Descriptive information of the tunnel interface
Tunnel0 Interface	Number of the tunnel interface
Maximum Transmit Unit	Maximum transmission unit on the tunnel
Encapsulation is TUNNEL	The encapsulation protocol is TUNNEL.
aggregation ID	ID of the link aggregation group applied to the tunnel. If the device does not support link aggregation group configuration or no link aggregation group is specified, the message "aggregation ID not set" is displayed.

Table 468 Description on the fields of the display interface tunnel command

Field	Description
Tunnel source	Source address of the tunnel interface
destination	Destination address of the tunnel interface
Tunnel keepalive	Whether the GRE keepalive function is enabled
Tunnel protocol/transport	Tunnel protocol/transport protocol
GRE key	Secret key for tunnel interfaces use
Checksumming of GRE packets	Whether GRE packet checksum is enabled
Last 300 seconds input	Amount of inbound traffic per second in the last five minutes, in bytes and in packets respectively
Last 300 seconds output	Amount of outbound traffic per second in the last five minutes, in bytes and in packets respectively
xxx packets input, xxx bytes	Cumulative amount of inbound traffic, in packets and in bytes respectively
input error	Number of wrong packets in all inbound packets
xxx packets output, xxx bytes	Cumulative amount of outbound traffic, in packets and in bytes respectively
output error	Number of wrong packets in all outbound packets

display ipv6 interface tunnel

Syntax **display ipv6 interface tunnel** *number*

View Any view

Parameter *number*: Tunnel interface number.

Description Use the **display ipv6 interface tunnel** command to display IPv6 information about a tunnel interface.

Example # Display IPv6 information about interface Tunnel0.

```
<Sysname> display ipv6 interface tunnel 0
Tunnel0 current state :UP
Line protocol current state :UP
IPv6 is enabled, link-local address is FE80::101:101
  Global unicast address(es):
    2002:101:101::1, subnet is 2002::/16
  Joined group address(es):
    FF02::1:FF01:101
    FF02::1:FF00:1
    FF02::2
    FF02::1
  MTU is 1500 bytes
  ND reachable time is 30000 milliseconds
  ND retransmit interval is 1000 milliseconds
  Hosts use stateless autoconfig for addresses
```

Table 469 Description on the fields of the display ipv6 interface tunnel command

Field	Description
Tunnel0 current state	Status of the physical layer of the tunnel interface, UP or DOWN
Line protocol current state	Status of the link layer of the tunnel interface, UP or DOWN
IPv6	Whether IPv6 is enabled on the tunnel interface
link-local address	Link-local address of the tunnel interface
Global unicast address(es)	Global unicast addresses of the tunnel interface
Joined group address(es)	Multicast addresses of the tunnel interface
MTU	Maximum transmission unit of the tunnel
ND reachable time	Interval during which the neighbor is considered reachable
ND retransmit interval	Neighbor discovery packet retransmission interval
Hosts use stateless autoconfig for addresses	Hosts use the stateless auto-configuration mode to acquire an IPv6 addresses.

encapsulation-limit

Syntax **encapsulation-limit** [*number*]

undo encapsulation-limit

View Tunnel interface view

Parameter *number*: Number of encapsulations in a tunnel, in the range 1 to 10.

Description Use the **encapsulation-limit** command to configure the maximum number of encapsulations on a tunnel.

Use the **undo encapsulation-limit** command to remove the configuration.

By default, the maximum encapsulation limit is 4.

The encapsulation limit applies to only IPv6 over IPv6 tunnels.

Example # Configure the encapsulation limit on a tunnel to 3.

```
<Sysname1> system-view
[Sysname1] interface tunnel 2
[Sysname-tunnel2] encapsulation-limit 3
```

gre checksum

Syntax **gre checksum**

undo gre checksum

View Tunnel interface view

Parameter None

Description Use the **gre checksum** command to enable the GRE packet checksum function so as to verify the validity of packets and discard those invalid packets.

Use the **undo gre checksum** command to disable the GRE packet checksum function.

By default, the GRE packet checksum function is disabled.

Related command: **interface tunnel**.

Example # Enable the GRE packet checksum function on the tunnel between Sysname1 and Sysname2.

```
<Sysname1> system-view
[Sysname1] interface tunnel 3
[Sysname1-Tunnel3] gre checksum
<Sysname2> system-view
[Sysname2] interface tunnel 2
[Sysname2-Tunnel2] gre checksum
```

gre key

Syntax **gre key** *key-number*

undo gre key

View Tunnel interface view

Parameter *key-number*: Secret key for the GRE tunnel interface use, in the range 0 to 4,294,967,295.

Description Use the **gre key** command to configure a secret key for a GRE tunnel interface. This weak security mechanism can prevent packets from being received mistakenly.

Use the **undo gre key** command to remove the configuration.

By default, no secret key is configured for a GRE tunnel interface.

Related command: **interface tunnel**

Example # Set the secret key for the GRE tunnel interfaces to 123 on Sysname1 and Sysname2.

```
<Sysname1> system-view
[Sysname1] interface tunnel 3
[Sysname1-Tunnel3] gre key 123
<Sysname2> system-view
[Sysname2] interface tunnel 2
[Sysname2-Tunnel2] gre key 123
```

interface tunnel

Syntax **interface tunnel** *number*

undo interface tunnel *number*

View System view

Parameter *number*: Number of a tunnel interface, in the range 0 to 1023. The volume of tunnels is subject to the total number of interfaces and the capacity of memory.

Description Use the **interface tunnel** command to create a tunnel interface and enter tunnel interface view.

Use the **undo interface tunnel** command to remove a tunnel interface.

By default, there is no tunnel interface on the device.

- Executing the **interface tunnel** command, you enter tunnel interface view if the tunnel interface exists.
- A tunnel interface number has only local significance. Therefore, both ends of a tunnel can have the same interface number or different interface numbers.

Related command: **source**, **destination**, **gre key**, **gre checksum**, and **tunnel-protocol** on page 887.

Example # Create an interface named Tunnel3 and enter its view.

```
<Sysname> system-view
[Sysname] interface tunnel 3
[Sysname-Tunnel3]
```

keepalive

Syntax **keepalive** [*seconds* [*times*]]

undo keepalive

View Tunnel interface view

Parameter *seconds*: Interval between transmitting keepalive packets, in the range 1 to 32,767 seconds. The default value is 10.

times: Maximum number of attempts for transmitting a keepalive packet, in the range 1 to 255. The default value is 3.

Description Use the **keepalive** command to enable the GRE keepalive function to detect the status of the tunnel interfaces and set the keepalive interval and the maximum number of attempts for transmitting a keepalive packet.

Use the **undo keepalive** command to disable the keepalive function.

By default, the GRE keepalive function is disabled.

With the GRE keepalive function enabled on a tunnel interface, the device sends GRE keepalive packets from the tunnel interface periodically. If no response is received from the peer within the specified interval, the device retransmits a keepalive packet. If the device still receives no response from the peer after a keepalive packet is transmitted for the maximum number of attempts, the local tunnel interface goes down and keeps down until it receives a keepalive acknowledgement packet from the peer.

Related command: **interface tunnel**.

Example # Set the GRE keepalive interval to 20 seconds and the maximum number of attempts for transmitting a keepalive packet to 5.

```
<Sysname> system-view
[Sysname] interface tunnel 0
[Sysname-Tunnel0] keepalive 20 5
```

source

Syntax **source** { *ip-address* | *ipv6-address* | *interface-type interface-number* }

undo source

View Tunnel interface view

Parameter *ip-address*: Source IPv4 address for a tunnel interface.

Ipv6-address: Source IPv6 address for a tunnel interface.

interface-type interface-number: Type and number of the source interface for a tunnel interface. The interface type can be Ethernet, VLAN, serial, ATM, tunnel, or loopback.

Description Use the **source** command to specify the source address or interface for a tunnel interface.

Use the **undo source** command to remove the configuration.

By default, no source address or interface is configured for a tunnel interface.

Note that:

- The source address of a tunnel interface is the address of the interface sending GRE packets and is usually the destination address of the peer tunnel interface.
- Two or more tunnel interfaces using the same encapsulation protocol must have different source addresses and destination addresses.

Related command: **interface tunnel** and **destination**.

Example # Create interface Tunnel5 and configure Serial2/0 (192.100.1.1) as its source interface.

```
<Sysname> system-view
[Sysname] interface tunnel 5
[Sysname-Tunnel5] source 192.100.1.1
```

Or

```
[Sysname-Tunnel5] source serial 2/0
```

tunnel-protocol gre

Syntax **tunnel-protocol gre** [**ipv6**]

undo tunnel-protocol

View Tunnel interface view

Parameter **ipv6**: Sets the tunnel mode to GRE over IPv6.

Description Use the **tunnel-protocol gre** command to set the GRE tunnel mode.

Use the **undo tunnel-protocol** to restore the default.

By default, the GRE tunnel mode is GRE over IPv4.

Without the **ipv6** keyword, the command sets the GRE tunnel mode to GRE over IPv4.

Select a tunnel mode according to the network topology and application. Note that both ends of a tunnel must be configured with the same tunnel mode. Otherwise, packet delivery will fail.

Related command: **interface tunnel**.

Example # Set the tunnel mode to GRE over IPv4 for the tunnel between Sysname1 and Sysname2.

```
<Sysname1> system-view
[Sysname1] interface tunnel 3
[Sysname1-Tunnel3] tunnel-protocol gre
<Sysname2> system-view
[Sysname2] interface tunnel 2
[Sysname2-Tunnel2] tunnel-protocol gre
```

104 L2TP CONFIGURATION COMMANDS

allow l2tp

Syntax **allow l2tp virtual-template** *virtual-template-number* **remote** *remote-name* [**domain** *domain-name*]

undo allow

View L2TP group view

Parameter *virtual-template-number*: Number of the virtual interface template for creating a virtual access interface, in the range of 0 to 1023.

remote-name: Name of the tunnel peer initiating a connection request, a case sensitive string of 1 to 30 characters.

domain-name: Name of the domain initiating a connection request, a string of 1 to 30 characters.

Description Use the **allow l2tp** command to specify the virtual interface template for receiving calls, the tunnel name of the LAC, and the domain name.

Use the **undo allow** command to remove the configuration.

By default, an LNS denies all incoming calls.

Note that:

- The **domain** *domain-name* combination is required in L2TP multi-instance applications.
- The **remote** *remote-name* combination is optional for L2TP group 1, the default L2TP group number. In other words, for L2TP group 1, the syntax of the command is **allow l2tp virtual-template** *virtual-template-number* [**remote** *remote-name*] [**domain** *domain-name*]. Computers with any name can initiate a tunneling request.
- If you specify the **remote** *remote-name* combination for L2TP group 1, L2TP group 1 will not serve as the default L2TP group.
- In Windows 2000 beta 2, if the local end name for a VPN connection is NONE, the peer name received by the router is NONE, too. A default L2TP group is set for the purpose of testing the tunnel connectivity or receiving the tunneling request initiated by such an unknown remote end.

- The **allow l2tp** command is available for only LNSs. If the tunnel name on the LAC is specified, ensure that it is the same as the tunnel name configured on the LAC.

Related command: **l2tp-group**.

Example # Accept the L2TP tunneling request initiated by the peer (LAC) of AS8010 and create a virtual access interface according to virtual template 1.

```
<Sysname> system-view
[Sysname] l2tp-group 2
[Sysname-l2tp2] allow l2tp virtual-template 1 remote AS8010
```

Specify L2TP group 1 as the default L2TP group, accept the L2TP tunneling request initiated by any peer, and create a virtual access interface based on virtual template 1.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] allow l2tp virtual-template 1
```

display l2tp session

Syntax **display l2tp session**

View Any view

Parameter None

Description Use the **display l2tp session** command to display information about L2TP sessions.

Related command: **display l2tp tunnel**.

Example # Display information about L2TP sessions.

```
<Sysname> display l2tp session
Total session = 1

 LocalSID       RemoteSID   LocalTID
 1          1           2
```

Table 470 Description on the fields of the display l2tp session command

Field	Description
Total session	Number of active sessions
LocalSID	Unique ID of the session at the local end
RemoteSID	Unique ID of the session at the remote end
LocalTID	Unique ID of the tunnel at the local end

display l2tp tunnel

Syntax **display l2tp tunnel**

View Any view

Parameter None

Description Use the **display l2tp tunnel** command to display information about L2TP tunnels.

Example # Display information about L2TP tunnels.

```
<Sysname> display l2tp tunnel
Total tunnel = 1

 LocalTID RemoteTID RemoteAddress Port  Sessions  RemoteName
 2        2284      11.1.1.1      1701  1         lns
```

Table 471 Description on the fields of the display l2tp tunnel command

Field	Description
Total tunnel	Number of active tunnels
LocalTID	Unique ID of the tunnel at the local end
RemoteTID	Unique ID of the tunnel at the remote end
RemoteAddress	IP address of the peer
Port	Port number of the peer
Sessions	Number of sessions within the tunnel
RemoteName	Name of the tunnel at the peer

interface virtual-template

Syntax **interface virtual-template** *virtual-template-number*

undo interface virtual-template *virtual-template-number*

View System view

Parameter *virtual-template-number*: Serial number for identifying the virtual interface template, in the range of 0 to 1023.

Description Use the **interface virtual-template** command to create a virtual interface template and enter its view.

Use the **undo interface virtual-template** command to remove a virtual interface template.

By default, no virtual interface template exists.

A virtual interface template is intended to provide parameters for virtual interfaces to be dynamically created by the router, such as logical MP interfaces and logical L2TP interfaces.

Related command: **allow l2tp**.

Example # Create virtual interface template 1 and enter virtual interface template view.

```
<Sysname> system-view
[Sysname] interface virtual-template 1
[Sysname-Virtual-Template1]
```

l2tp enable

Syntax **l2tp enable**

undo l2tp enable

View System view

Parameter None

Description Use the **l2tp enable** command to enable the L2TP function.

Use the **undo l2tp enable** command to disable the L2TP function.

By default, the L2TP function is disabled.

You must enable L2TP before performing L2TP configurations.

Related command: **l2tp-group**.

Example # Enable the L2TP function.

```
<Sysname> system-view
[Sysname] l2tp enable
```

l2tp sendaccm enable

Syntax **l2tp sendaccm enable**

undo l2tp sendaccm enable

View System view

Parameter None

Description Use the **l2tp sendaccm enable** command to enable an LNS to include ACCM in control messages.

Use the **undo l2tp enable** command to disable the function.

By default, an LNS includes ACCM in control messages.

Example # Disable the ACCM function.

```
<Sysname> system-view
[Sysname] undo l2tp sendaccm enable
```

l2tpmoreexam enable

Syntax **l2tpmoreexam enable**

undo l2tpmoreexam enable

View System view

Parameter None

Description Use the **l2tpmoreexam enable** command to enable the L2TP multi-instance function.

Use the **undo l2tpmoreexam enable** command to disable the L2TP multi-instance function.

By default, the L2TP multi-instance function is disabled.

Note that this command is available for only LNSs.

Related command: **l2tp enable**.

Example # Enable the L2TP multi-instance function for the router.

```
<Sysname> system-view
[Sysname] l2tpmoreexam enable
```

l2tp-group

Syntax **l2tp-group** *group-number*

undo l2tp-group *group-number*

View System view

Parameter *group-number*: Number for identifying the L2TP group, in the range of 1 to 1000.

Description Use the **l2tp-group** command to create an L2TP group and enter its view.

Use the **undo l2tp-group** command to remove an L2TP group.

By default, no L2TP group exists.

When you use the **undo l2tp-group** command to remove an L2TP group, all configuration information associated with the group will be deleted.

Related command: **allow l2tp** and **start l2tp**.

Example # Create an L2TP group numbered 2 and enter its view.

```
<Sysname> system-view
[Sysname] l2tp-group 2
[Sysname-l2tp2]
```

mandatory-chap

Syntax **mandatory-chap**

undo mandatory-chap

View L2TP group view

Parameter None

Description Use the **mandatory-chap** command to force the LNS to perform a CHAP authentication of the user.

Use the **undo mandatory-chap** command to disable CHAP authentication on the LNS.

By default, an LNS does not perform CHAP authentication of users.

An LNS authenticates the client in addition to the proxy authentication that occurs at the LAC for higher security. If the **mandatory-chap** command is used, two authentications are performed for the clients connected to the VPN through an initialized tunnel of the NAS: one on the NAS side and the other on the LNS side. Some PPP clients may not support the second authentication. In this case, the local CHAP authentication will fail.

Related command: **mandatory-lcp**.

Example # Perform CHAP authentication by force.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] mandatory-chap
```

mandatory-lcp

Syntax **mandatory-lcp**

undo mandatory-lcp

View L2TP group view

Parameter None

Description Use the **mandatory-lcp** command to force an LNS to perform LCP negotiation with users.

Use the **undo mandatory-lcp** command to disable the LCP negotiation.

By default, an LNS does not perform LCP negotiation with users.

When starting a PPP session, a client of NAS-initialized VPN will first negotiate with the network access server (NAS) for LCP parameters. If the negotiation succeeds, the NAS initializes a tunnel and then transfers the negotiated results to the LNS. Then the LNS verifies whether the client is valid depending on the proxy authentication information. You can use the **mandatory-lcp** command to force the LNS to perform LCP re-negotiation for the client. But the proxy authentication information of the NAS may be neglected. Some PPP clients may not support LCP re-negotiation. In this case, the LCP re-negotiation will fail.

Related command: **mandatory-chap**.

Example # Perform LCP negotiation by force.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] mandatory-lcp
```

reset l2tp tunnel

Syntax **reset l2tp tunnel** { *remote-name* | *tunnel-id* }

View User view

Parameter *remote-name*: Name of the tunnel at the remote end.

tunnel-id: Local ID of the tunnel, in the range of 1 to 8191.

Description Use the **reset l2tp tunnel** command to disconnect one or more specified tunnels and all sessions of the tunnels.

Note that:

- A tunnel disconnected by force can be re-established when a client makes a call.
- If you specify a tunnel name, all tunnels with the name, if any, will be disconnected. If no tunnel with the name exists, nothing happens.
- If you specify a tunnel ID, only the tunnel with the ID is disconnected.

Related command: **display l2tp tunnel**.

Example # Disconnect all tunnels with the remote name of AS8010.

```
<Sysname> reset l2tp tunnel AS8010
```

start l2tp

Syntax **start l2tp ip** *ip-address*&<1-5> { **domain** *domain-name* | **fullusername** *user-name* }

undo start

View L2TP group view

Parameter *ip-address*&<1-5>: IP addresses of the tunnel peers (LNSs). &<1-5> means that you can specify up to five IP addresses.

domain-name: Name of the domain initiating a connection request, a case sensivive string of 1 to 30 characters.

user-name: Full qualified name of the user initiating a connection request, a case sensitive string of 1 to 32 characters.

Description Use the **start l2tp** command to enable the device to initiate tunneling requests to one or more IP addresses for one or more specified VPN users.

Use the **undo start** to remove the specified triggering condition.

Note that:

- The **start l2tp** command is available for only LACs.
- An LAC can initiate tunneling requests for users in a specified domain. For example, if the domain name of a company is aabbcc.net, users with such a domain name are considered VPN users.
- You can specify a single VPN user by giving the fully qualified name of the user.
- When an LAC detects a VPN user, it initiates an L2TP tunneling request to LNSs one by one in their configuration order until it receives the acknowledgement of an LNS, which is considered the tunnel peer.

Example # Initiate L2TP tunneling requests to LNS 202.38.168.1 for users in domain aabbcc.net.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] start l2tp ip 202.38.168.1 domain aabbcc.net
```

tunnel authentication

Syntax **tunnel authentication**

undo tunnel authentication

View L2TP group view

Parameter None

Description Use the **tunnel authentication** command to enable the L2TP tunnel authentication function.

Use the **undo tunnel authentication** command to disable the L2TP tunnel authentication function.

By default, L2TP tunnel authentication function is enabled.

Generally, authentication is required at both ends of a tunnel for the sake of security. However, you can disable the authentication when you check network connectivity or it is required to receive tunneling requests from unknown tunnel peers.

Example # Disable L2TP tunnel authentication.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] undo tunnel authentication
```

tunnel avp-hidden

Syntax **tunnel avp-hidden**

undo tunnel avp-hidden

View L2TP group view

Parameter None

Description Use the **tunnel avp-hidden** command to specify to transfer attribute value pair (AVP) data in hidden mode.

Use the **undo tunnel avp-hidden** command to restore the default.

By default, AVP data is transferred over a tunnel in plain text mode.

Note that:

- Some parameters of L2TP are transferred in AVP data. You can use the **tunnel avp-hidden** command to transfer AVP data in hidden mode for higher security.
- The **tunnel avp-hidden** command is available for only LACs.

Example # Transfer AVP data in hidden mode.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] tunnel avp-hidden
```

tunnel flow-control

Syntax **tunnel flow-control**

undo tunnel flow-control

View L2TP group view

Parameter None

Description Use the **tunnel flow-control** command to enable the L2TP tunnel flow control function.

Use the **undo tunnel flow-control** command to disable the L2TP tunnel flow control function.

By default, the L2TP tunnel flow control function is disabled.

Example # Enable the L2TP tunnel flow control function.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] tunnel flow-control
```

tunnel name

Syntax **tunnel name** *name*

undo tunnel name

View L2TP group view

Parameter *name*: Name for the tunnel at the local end, a string of 1 to 30 characters.

Description Use the **tunnel name** command to specify the name of a tunnel at the local end.

Use the **undo tunnel name** command to restore the default.

By default, a tunnel takes the system name of the device as its name at the local end.

Related command: **sysname** on page 2423.

Example # Specify the local name for a tunnel as itsme.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] tunnel name itsme
```

tunnel password

Syntax **tunnel password** { **simple** | **cipher** } *password*

undo tunnel password

View L2TP group view

Parameter **simple**: Displays the password in plain text.

cipher: Displays the password in cipher text.

password: Password for tunnel authentication, case sensitive. If you specify the **simple** keyword, you can enter a password only in plain text. If you specify the **cipher** keyword, you can enter a password in either plain text or cipher text. A plain text password is a string of 1 to 16 characters that contains no space, for example, aabbcc. A cipher text password consists of 24 characters, for example, _(TT8F)Y5SQ=^Q'MAF4<1!!.

Description Use the **tunnel password** command to specify the password for tunnel authentication.

Use the **undo tunnel password** command to remove the configuration.

By default, the password for tunnel authentication is null.

Example # Set the password for tunnel authentication to yougotit, specifying to display the password in cipher text.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] tunnel password cipher yougotit
```

tunnel timer hello

Syntax **tunnel timer hello** *hello-interval*

undo tunnel timer hello

View L2TP group view

Parameter *hello-interval*: Interval at which the LAC or the LNS sends Hello packets when receiving no packets, in the range of 60 to 1,000 seconds.

Description Use the **tunnel timer hello** command to set the hello interval in sending hello packets in a tunnel.

Use the **undo tunnel timer hello** command to restore the default.

By default, the interval is 60 seconds.

You can set different hello intervals for the LNS and LAC.

Example # Set the hello interval to 99 seconds.

```
<Sysname> system-view
[Sysname] l2tp-group 1
[Sysname-l2tp1] tunnel timer hello 99
```

105 TRAFFIC POLICING (TP) CONFIGURATION COMMANDS

display qos car interface

Syntax **display qos car interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos car interface** command to view parameter configuration and running statistics of CAR at each or all interfaces.

If no interface is specified, CAR configuration and running statistics of all interfaces will be displayed.

Examples # Display the CAR parameter configuration information and running statistic information on each interface.

```
<Sysname> display qos car interface Ethernet1/0
Interface: Ethernet1/0
Direction: Inbound
  Rule(s): If-match Any
  CIR 10 (kbps),  CBS 2000 (byte),  EBS 0 (byte)
  Green Action: pass
  Red Action : discard
  Green: 0/0 (Packets/Bytes)
  Red  : 0/0 (Packets/Bytes)

Direction: Outbound
  Rule(s): If-match ACL  2002
  CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
  Green Action: pass
  Red Action : discard
  Green: 0/0 (Packets/Bytes)
  Red  : 0/0 (Packets/Bytes)
```

Table 472 Description on the fields of the display qos car command

Filed	Description
Interface	Interface name, consisting of interface type and interface number
Direction	Specifies the direction of traffic policing.
Rule(s)	Matching rules of packets
CIR	Committed Information Rate, in kbps

Table 472 Description on the fields of the display qos car command

Filed	Description
CBS	Committed Burst Size, i.e. the depth of token bucket carrying burst traffic, in byte
EBS	Excess Burst Size, i.e. the size of the burst traffic exceeding the committed traffic in dual-token bucket algorithm, in byte
Green Action	Operation performed for packets sent at the rate below CIR
Red Action	Operation performed for packets sent at the rate above CIR
Green	Number of byte number of packets sent at the rate below CIR
Red	Number of byte number of packets sent at the rate above CIR

display qos carl

Syntax **display qos carl** [*carl-index*]

View Any view

Parameters *carl-index*: Committed Access Rate List (CARL) number, in the range 1 to 199.

Description Use the **display qos carl** command to view a certain rule or all the rules of CARL.

If *carl-index* is not specified, all rules of CARL will be displayed.

Examples # Display the first rule of CAR list.

```
<Sysname> display qos carl 1
Current CARL Configuration:
List  Params
------------------------------------------------------
1     MAC Address 0001-0001-0001
```

Table 473 Description on the fields of the display qos carl command

Field	Description
List	List of rule number
Params	Matching rules of packet

qos car

Syntax **qos car** { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-numbe*r | **carl** *carl-index* } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action*] [**red** *action*]

undo qos car { **inbound** | **outbound** } { **any** | **acl** [**ipv6**] *acl-number* | **carl** *carl-index* }

View Interface view

Parameters **inbound**: Limits rate for the packets received by the interface.

outbound: Limits rate for the packets sent by the interface.

any: Limits rates for all packets that match any rules.

acl *acl-number*: Limits the rate of packets matching the IPv4 ACL, with *acl-number* being the IPv4 ACL number. It ranges from 2000 to 3999.

acl ipv6 *acl-number*: Limits the rate of packets matching the IPv6 ACL, with *acl-number* being the IPv6 ACL number. It ranges from 2000 to 3999.

carl *carl-index*: Limits the rate of packets matching the CARL, with *carl-index* being the CARL number, in the range 1 to 199.

cir *committed-information-rate*: CIR, in the range 8 to 1000000 kbps.

cbs *committed-burst-size*: CBS, in the range 1875 to 19375000 bytes, with the default value being the traffic passed at CIR in 500 milliseconds. If the traffic passed at CIR in 500 milliseconds is lower than 1875, 1875 is taken as the default value.

ebs *excess-burst-size*: EBS, in the range 0 to 19375000 bytes. It defaults to 0.

green: Action taken on the packets when the traffic rate conform to CIR. The default action is **pass**.

red: Action taken on the packets when the traffic rate does not conform to CIR. The default action is **discard**.

action: Action taken on a packet, which can be:

continue: Has it to be dealt with by the next CAR policy.

discard: Discards the packet.

pass: Sends the packet.

remark-dscp-continue *new-dscp*: Remarks the packet with a new DSCP value and hands it over to the next CAR policy. Ranges from 0 to 63. When it is displayed in characters, its value can be **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, ef.**

remark-dscp-pass *new-dscp*: Remarks the packet with a new DSCP value and forwards the packet. Ranges from 0 to 63. When it is displayed in characters, its value can be **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, ef.**

remark-prec-continue *new-precedence*: Remarks the packet with a new IP precedence and hands it over to the next CAR policy. Ranges from 0 to 7.

remark-prec-pass *new-precedence*: Remarks the packet with a new IP precedence and forwards the packet. Ranges from 0 to 7.

Description Use the **qos car** command to implement CAR policy on an interface.

Use the **undo qos car** command to remove a certain CAR policy at the interface.

You can configure several CAR policies by using the command for several times. And the executing order of the policies depends on the configuration order.

Execute the command in interface view, and the setting is valid on the current interface only.

Examples # Configure traffic policing for outbound packets that conform to CARL rule 1 at the interface Ethernet1/0. The normal traffic is 200 kbps. The burst size, twice of the normal traffic, is allowed at the first time; then packets are normally transmitted when the rate is less than or equal to 200 kbps. When the rate is larger than 200 kbps, packets will be transmitted after their precedence is changed to 0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos car outbound carl 1 cir 200 cbs 50000 ebs
0 green pass red remark-prec-pass 0
```

qos carl

Syntax **qos carl** *carl-index* { **precedence** *precedence-value* | **mac** *mac-address* | **dscp** *dscp-list* }

undo qos carl *carl-index*

View System view

Parameters *carl-index*: CAR list number, in the range 1 to 199.

precedence-value: Precedence, in the range 0 to 7.

mac-address: Hexadecimal MAC address.

dscp-list: DSCP value list. When it is displayed by a number, it ranges from 0 to 63; when it is displayed as a character, it can be valued **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default** and **ef**.

Description Use the **qos carl** command to establish or modify a CARL.

Use the **undo qos carl** command to delete a CARL.

You can establish a CARL based on IP precedence, or MAC address.

For different *carl-index*, the repeat execution of this command will create multiple CARLs, and for the same *carl-index*, such undertaking will modify the parameters of the CARL.

You can define eight **precedence** values at most. If the same **precedence** is specified for several times, the system by default regards that only one **precedence** value has been specified. The **precedence** values are related to one another in the way of "OR".

You can define eight DSCP values at most. If the same DSCP is specified for several times, the system by default regards that only one DSCP value has been specified. The DSCP values are related to one another in the way of "OR".

Examples # Configure CARL rule 1 with packet precedence 7.

```
<Sysname> system-view
[Sysname] qos carl 1 precedence 7
```

106 TRAFFIC SHAPING CONFIGURATION COMMANDS

display qos gts interface

Syntax **display qos gts interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos gts interface** command to view GTS configuration and accounting information of certain interface or all interfaces.

If no interface is specified, the GTS configuration and running statistics of all interfaces will be displayed.

Examples # Display GTS configuration and accounting information of all interfaces.

```
<Sysname> display qos gts interface
Interface: Ethernet1/0
Rule(s): If-match ACL  2001
CIR  200(kbps),  CBS  50000(byte),   EBS  0(byte)
 Queue Length: 100 (Packet)
Queue Size: 70 (Packet)
Passed:  0/0 (Packets/Bytes)
Discarded:  0/0 (Packets/Bytes)
Delayed:  0/0 (Packets/Bytes)
```

Table 474 Description on the fields of the display qos gts command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Rule(s)	Matching rules of packets, which can be any of the three
CIR	Committed Information Rate, in kbps
CBS	Committed Burst Size, i.e. the depth of token bucket carrying burst traffic, in byte
EBS	Excess Burst Size, i.e. the size of the burst traffic exceeding the committed traffic in dual-token bucket algorithm, in byte
Queue Length	Length of packets that a buffer queue can hold.
Queue Size	Number of packets in the current buffer
Passed	Number and byte number of passed packets.

Table 474 Description on the fields of the display qos gts command

Field	Description
Discarded	Number and byte number of discarded packets.
Delayed	Number and byte number of delayed packets.

qos gts

Syntax **qos gts** { **any** | **acl** *acl-number* } **cir** *committed-information-rate* [**cbs** *committed-burst-size*] [**ebs** *excess-burst-size*] [**queue-length** *queue-length*]]

undo qos gts { **any** | **acl** *acl-number* | **queue** *queue-number* }

View Interface view

Parameters **any**: Performs TS on all the packets.

acl *acl-number*: Performs TS on packets matching the ACL. *acl-number* is the ACL number, in the range 2000 to 3999.

cir *committed-information-rate*: CIR, in the range 8 to 1000000.

cbs *committed-burst-size*: CBS, in the range 1875 to 19375000 bytes, with the default value being the traffic passed at CIR in 500 milliseconds. If the traffic passed at CIR in 500 milliseconds is lower than 1875, 1875 is taken as the default value.

ebs *excess-burst-size*: EBS, i.e. size of the burst traffic exceeding the committed traffic in dual-token bucket algorithm, in the range 0 to 19375000 bytes. It defaults to 0, that is, only one token bucket is used for policing.

queue-length *queue-length*: The maximum length of the buffer, in the range 1 to 1024. By default, *queue-length* is 50.

Description Use the **qos gts** command to set shaping parameters for all or a specified type of traffic and perform traffic shaping.

Use the **undo qos gts** command to remove the shaping configuration for all or a specified type of traffic.

qos gts acl is used to set shaping parameters for the packets that conforms to certain ACL. Different ACLs can be used to set shaping parameters for different packets.

qos gts any is used to set shaping parameters for all packets.

The **qos gts acl** and **qos gts any** cannot be used at the same time. Only one can be used each time.

By default, no shaping parameter is set on the interface.

Execute the command in interface view, and the setting is effective on the current interface only.

Related commands: **acl** on page 2087.

IPv6 is not supported for traffic shaping for software forwarding.

Examples # Configure traffic shaping for the packets that conform to ACL rule 2001 at the Ethernet1/0 interface. The normal traffic is 200 kbps. The burst size, twice of the normal traffic (50000 bytes), is allowed at the first time. Then packets are normally transmitted when the traffic is less than or equal to 200 kbps. When the rate is larger than 200 kbps, packets will be added to the buffer queue, which is 100 long.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] qos gts acl 2001 cir 200 cbs 50000 ebs 0 queue
-length 100
```

107 LINE RATE CONFIGURATION COMMANDS

display qos lr interface

Syntax **display qos lr interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos lr interface** command to view LR configuration and statistics of an interface or all interfaces.

If no interface is specified, the LR configuration and running statistics of all interfaces will be displayed.

Examples # Display LR configuration and statistics information of all interfaces.

```
<Sysname> display qos lr interface
Interface: Ethernet1/0

Direction: Outbound
 CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
 Passed : 0/0 (Packets/Bytes)
 Delayed: 0/0 (Packets/Bytes)
 Active Shaping:  NO
Direction: Inbound
 CIR 10 (kbps),  CBS 1875 (byte),  EBS 0 (byte)
 Passed : 0/0 (Packets/Bytes)
 Delayed: 0/0 (Packets/Bytes)
 Active Shaping:  NO
```

Table 475 Description on the fields of the display qos lr command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Direction	Indicates the direction of line rate, i.e. inbound or outbound
CIR	Committed Information Rate, in kbps
CBS	Committed Burst Size, i.e. the depth of token bucket carrying burst traffic, in byte
EBS	Excess Burst Size, i.e. the size of the burst traffic exceeding the committed traffic in dual-token bucket algorithm, in byte

Table 475 Description on the fields of the display qos lr command

Field	Description
Passed	Number and byte number of passed packets.
Delayed	Number and byte number of delayed packets.
Active Shaping	Whether the current LR configuration is activated or not.

qos lr (interface view)

Syntax **qos lr outbound cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

undo qos lr { **inbound** | **outbound** }

View Interface view

Parameters **outbound**: Configures LR for data streams sent by the interface.

cir *committed-information-rate*: CIR, in the range 8 to 1000000 kbps.

cbs *committed-burst-size*: CBS, with the default value being the traffic passed at CIR in 500 milliseconds. If the traffic passed at CIR in 500 milliseconds is lower than 1875, 1875 is taken as the default value.

ebs *excess-burst-size*: EBS, i.e. size of the burst traffic exceeding the committed traffic in dual-token bucket algorithm, in byte. It defaults to 0, that is, only one token bucket is used for policing.

Description Use the **qos lr** command to limit the transmitting or receiving rate of the interface.

Use the **undo qos lr** command to remove the limit.

Execute the command in interface view, and the setting is effective on the current interface only.

Examples # Limit packet-forwarding rate of interface Ethernet1/0 to the normal rate 20 kbps. The CBS value is 2000 bytes and the EBS value is 0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos lr outbound cir 20 cbs 2000 ebs 0
```

qos lr (layer 2 interface view or port group view)

Syntax **qos lr** { **inbound outbound** } **cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]]

undo qos lr { **inbound outbound** }

View Layer 2 module interface view, port group view

Parameters **inbound**: Configures LR for data streams received by the interface. For a device which cannot be installed with an external interface module or when the number of the interfaces is 4 or 9, this argument is not supported.

outbound: Configures LR for data streams sent by the interface.

cir *committed-information-rate*: CIR, with the value being 128, 256, 512, 1024, 2048, 4096 or 8192 kbps for a device which cannot be installed with an external interface module or when the number of the interfaces on a layer 2 module is 4 or 9. If the number of interfaces on a layer 2 module is 16, 24 or 48, the value ranges from 64 to 1000000, in steps of 64 kbps.

cbs *committed-burst-size*: CBS, with the value being 4096, 8192, 16384, 32768, 65536, 131072, 262144, 524288 bytes when the number of the interfaces on a layer 2 module is 16, 24 or 48. It defaults to 4096 bytes. If the **cbs** *committed-burst-size* configured by the user is not a specified one, the system automatically selects the nearest one. For a device which cannot be installed with an external interface module or when the number of the interfaces is 4 or 9, this argument is not supported.

ebs *excess-burst-size*: This argument is not supported on the interface on a layer 2 module for a device which cannot be installed with an external interface module or when the number of the interfaces on the layer 2 module is 4, 9, 16, 24 or 48.

Description Use the **qos lr** command to limit the transmitting or receiving rate of the interface.

Use the **undo qos lr** command to remove the limit.

Execute the command in interface view, and the setting is valid on the current interface only. Port group is supported when the number of the interfaces on a layer 2 module is 16, 24 or 48. If this command is executed in port group view, the setting is valid on all ports.

Examples # Limit packet-forwarding rate of interface Ethernet1/0 to the normal rate 64 kbps. The CBS value is 8192 bytes.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos lr outbound cir 64 cbs 8192
```

108 DEFINING CLASS COMMANDS

display traffic classifier

Syntax **display traffic classifier** { **system-defined** | **user-defined** } [*tcl-name*]

View Any view

Parameters **system-defined**: Class pre-defined by the system.

user-defined: Class pre-defined by the user.

tcl-name: Class name, a string of characters in the range 1 to 31.

Description Use the **display traffic classifier** command to view the configuration information about the class.

If no class name is specified, this command displays information for all system-predefined classes or all user-predefined classes.

Examples # Display configuration information about the class.

```
<Sysname> display traffic classifier user-defined
User Defined Classifier Information:
 Classifier: USER1
  Operator: AND
  Rule(s) : if-match ip-precedence 5

 Classifier: database
  Operator: AND
  Rule(s) : if-match acl 3131
            if-match inbound-interface Ethernet1/0
```

Table 476 Description on the fields of display traffic classifier user-defined

Field	Description
User Defined Classifier Information	Class type: user-defined
Classifier	Class name and content: including multiple types
Operator	Logical relationship between classification rules
Rule	Classification rule

if-match

Syntax **if-match** [**not**] *match-criteria*

undo if-match [**not**] *match-criteria*

View Class view

Parameters **not**: Specifies to be the rule that does not match the specified matching rule.

match-criteria: Class match rules. The values are as follow:

Table 477 Values of matching rules for class

Value	Description
acl [**ipv6**] { *acl-number* | **name** *acl-name* }	Define ACL matching rule The *acl-number* argument is the ACL number, which is in the range of 2000 to 5999 for IPv4 ACLs and in the range of 2000 to 3999 and 10000 to 42767 for IPv6 ACLs. The *acl-name* argument is the ACL name. It is a non case-sensitive string of 1 to 32 characters. It must begin with a to z or A to Z. It cannot be **all** in order to avoid confusion.
any	Define matching rule for all packets.
classifier *tcl-name*	Define QoS matching rule; the class name is tcl-name, which is the type of a string of characters in the range 1 to 31.
customer-vlan-id *vlan-id-list*	Define customer VLAN ID matching rule; vlan-id-list is the list of VLAN ID, and up to 8 IDs can be input. The ID is valued in the range 1 to 4094.
destination-mac *mac-address*	Define destination MAC address matching rule.
dscp *dscp-list*	Define DSCP matching rule; dscp-list is the list of DSCP values, and up to eight DSCP values can be input. The DSCP value is in the range 0 to 63. When it is displayed in characters, its value can be **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, ef.**
inbound-interface *interface-type interface-number*	Define inbound interface matching rule; interface-type interface-number specifies the interface by type and number.
ip-precedence *ip-precedence-list*	Define IP precedence matching rule; ip-precedence-list is the list of ip-precedence and up to eight ip precedence can be input. The ip-precedence is valued in the range 0 to 7.
mpls-exp *exp-list*	Define MPLS EXP precedence matching rule; exp-list is the list of EXP and up to eight EXPs can be input. The EXP is valued in the range 0 to 7.
protocol *protocol-name*	Define protocol matching rule; protocol-name is valued to be **bgp**, **bittorrent**, **citrix**, **cuseeme**, **dhcp**, **dns**, **edonkey, egp, eigrp**, **exchange**, **fasttrack**, **finger**, **ftp**, **gnutella**, **gopher**, **gre**, **h323**, **http**, **icmp**, **igmp**, **imap**, **ip**, **ipinip**, **ipsec**, **ipv6**, **irc**, **Kerberos**, **l2tp**, **ldap**, **mgcp**, **napster**, **netbios**, **netshow**, **nfs**, **nntp**, **notes**, **novadign**, **ntp**, **pcanywher**, **pop3**, **pptp**, **printer**, **rcmd**, **rip**, **rsvp**, **rtcp**, **rtp**, **rtsp**, **secure-ftp**, **secure-http, secure-ima**, **secure-irc**, **secure-ldap**, **secure-nntp**, **secure-pop**, **secure-teln**, **sip**, **skinny**, **smtp**, **snmp**, **socks**, **sqlnet**, **sqlserver**, **ssh**, **streamwor**, **sunrpc**, **syslog**, **telnet**, **tftp**, **unknown-o**, **unknown-t**, **unknown-u**, **vdolive**, **winmx**, **xwindows**.

Table 477 Values of matching rules for class

Value	Description
rtp start-port *start-port-number* **end-port** *end-port-number*	Define RTP port matching rule. start-port-number is the starting RTP port number which is valued in the range 2000 to 65535; end-port-number is the ending RTP port number which is valued in the range 2000 to 65535.
qos-local-id *local-id-value*	Define qos-local-id matching rule; *local-id-value* is the local QoS ID in the range 1 to 4095.
source-mac *mac-address*	Define source MAC address matching rule.

*You can also use the **undo if-match** [**not**] command in the following syntax to change the ACL used for traffic classification to a new one: **undo if-match** [**not**] **acl** [**ipv6**] { acl-number | **name** acl-name } [**update acl** [**ipv6**] { acl-number | **name** acl-name }].*

Description

Use the **if-match** command to define the matching rule of all packets that match the specified matching rules.

Use the **undo if-match** command to delete the matching rules.

Use the **if-match not** command to define the match rule of all packets that do not match the specified matching rules.

Use the **undo if-match not** command to delete the matching rules.

When defining the rules, take the following into consideration:

1 Define ACL matching rule

- If the ACL referenced in a class is not created, the class cannot be applied.
- A class can reference the same ACL by ACL name and ACL number respectively.

2 Define destination MAC address matching rule.

- For a class, you can configure multiple commands which cannot be overwritten.
- The match rules of the destination MAC address are only meaningful for interfaces of Ethernet type.

3 Define source MAC address matching rule.

- For a class, you can configure multiple commands which cannot be overwritten.
- The match rules of the source MAC address are only meaningful for interfaces of Ethernet type.

4 Define matching rule for the class.

When defining both logical AND and logical OR match rules for a class, you may use this command.

For example, to define classA to match rule1 & rule2 | rule3 requires to define:

- traffic classifier classB operator and

- if-match rule 1
- if-match rule 2
- traffic classifier classA operator or
- if-match rule 3
- if-match classifier classB

For a class, you can configure multiple commands which cannot be overwritten.

5 Define DSCP matching rule.

- For a class, you can configure multiple commands which cannot be overwritten. The DSCP values specified by them are automatically arranged in ascending order. Only when the specified DSCP values are identical with those in the rule (sequence may be different) can the command be deleted.
- You may configure up to eight DSCP values in one command. If multiple DSCPs of the same value are specified, the system regards them as one. Relation between different DSCP values is "OR".

6 Define 802.1p priority matching rule.

For a class, you can configure multiple commands which cannot be overwritten. The 802.1p priority values specified by them are automatically arranged in ascending order. Only when the specified 802.1p priority values are identical with those in the rule (sequence may be different) can the command be deleted.

You may configure up to eight 802.1p priority values in one command. If multiple 802.1p priorities of the same value are specified, the system regards them as one. Relation between different 802.1p priority values is "OR".

7 Define inbound interface matching rule.

- For a class, you can configure multiple commands which cannot be overwritten.
- Before defining this matching rule, make sure that the interface exists. If the specified interface is a dynamic one, removing the interface can delete the rule.
- Supported interfaces: ATM, Ethernet, serial port, Tunnel, VT, etc.

8 Define IP precedence matching rule

- For a class, you can configure multiple commands which cannot be overwritten. When the command is configured, the ip-precedence values will be arranged automatically in ascending order. Only when the specified ip-precedence values are identical with those in the rule (sequence may be different) can the command be deleted.
- You may configure up to eight ip-precedence values in one command. If multiple ip precedence of the same value are specified, the system regards them as one. Relation between different ip-precedence values is "OR".

9 Define MPLS EXP precedence matching rule.

- For a class, you can configure multiple commands which cannot be overwritten. When the command is configured, the MPLS EXP precedence values will be arranged automatically in ascending order. Only when the

specified MPLS EXP precedence values are identical with those in the rule (sequence may be different) can the command be deleted.

- You may configure up to eight MPLS EXP precedence values in one command. If multiple MPLS EXP precedences of the same value are specified, the system regards them as one. Relation between different local priorities is "OR".
- The MPLS EXP field is specific to MPLS packets, so this matching rule is effective for only the MPLS packets.
- As for software forwarding QoS, MPLS packets do not support IP-related matching rules.

10 Define RTP port matching rule.

- This command can match RTP packets in the range of specified RTP port number, i.e., to match packets of even UDP port numbers between *<starting-port-number>* and < *end-port-number* >.
- If this command is frequently configured under one class, the last configuration will take effect.

11 Define VLAN ID matching rule.

- For a class, you can configure multiple commands which cannot be overwritten. When the command is configured, the *vlan-id* values will be arranged automatically in ascending order. Only when the specified VLAN ID values are identical with those in the rule (sequence may be different) can the command be deleted.
- You may multiple VLAN ID values in one command. If multiple VLAN IDs of the same value are specified, the system regards them as one. Relation between different VLAN IDs is "OR".

Related commands: **traffic classifier**.

Examples # Define the packet whose class match protocol is not IP.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match not protocol ip
```

Define that the matching rule of class1 is to match the packets with the destination MAC address 0050-ba27-bed3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match destination-mac 0050-ba27-bed3
```

Define that the matching rule of class2 is to match the packets with the destination MAC address 0050-ba27-bed2.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match source mac 0050-ba27-bed2
```

Define a class to match ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl 3101
```

Define a class to match the ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match acl name flow
```

Define a class to match IPV6 ACL 3101.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ipv6 acl 3101
```

Define a class to match the IPv6 ACL named **flow**.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ipv6 acl name flow
```

Define matching rule for all packets.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match any
```

Define match rule of class2 and class1 must be used. Therefore, class1 is configured first. The match rule of class1 is the IP precedence is 5.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 5
```

Define the packet whose class is class2, match rule is class1 and destination MAC address is 0050-BA27-BED3.

```
<Sysname> system-view
[Sysname] traffic classifier class2
[Sysname-classifier-class2] if-match classifier class1
[Sysname-classifier-class2] if-match destination-mac 0050-BA27-BED3
```

Define the match rule of class1 as matching the packets with the DSCP value as 1, 6 or 9.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match dscp 1 6 9
```

Define that the class matches the packets entering from Ethernet1/0.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match inbound-interface Ethernet1/0
```

Define the match rule of class1 as matching the packets with the DSCP value as 1 or 6.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match ip-precedence 1 6
```

Define the packet whose class match protocol is IP.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match protocol ip
```

Define the match rule of class1 as matching the packets whose RTP port number is the even UDP port number between 16384 and 32767.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match rtp start-port 16384 end-port 3
2767
```

Define the class to match qos-local-id 3.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] if-match qos-local-id 3
```

Change the ACL of class 1 used for traffic classification from ACL 2008 to ACL 2009.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] undo if-match acl 2008 update 2009
```

traffic classifier

Syntax **traffic classifier** *tcl-name* [**operator** { **and** | **or** }]

undo traffic classifier *tcl-name*

View System View

Parameters **and**: Specifies the relation between the rules in the class as logic AND. That is, the packet that matches all the rules belongs to this class.

or: Specifies the relation between the rules in the class as logic OR. That is, the packet that matches any one of the rules belongs to this class.

tcl-name: Class name, a string of characters in the range 1 to 31.

Description Use the **traffic classifier** command to define a class and enter the class view.

Use the **undo traffic classifier** command to delete a class.

By default, the relation is **operator and**.

tcl-name shall not be the classes pre-defined by the system. The classes defined by the system include: default-class, ef, af1, af2, af3, af4, ip-prec0, ip-prec1, ip-prec2, ip-prec3, ip-prec4, ip-prec5, ip-prec6, ip-prec7, mpls-exp0, mpls-exp1, mpls-exp2, mpls-exp3, mpls-exp4, mpls-exp5, mpls-exp6, and mpls-exp7.

Related commands: **qos policy**, **qos apply policy (interface view)**, **classifier behavior**.

Examples # Define a class named as class1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1]
```

109 DEFINING TRAFFIC BEHAVIOR COMMANDS

car

Syntax **car cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size*]] [**green** *action*] [**red** *action*]

undo car

View Traffic behavior view

Parameters **cir** *committed-information-rate*: Committed information rate, in the range 8 to 1000000 kbps.

cbs *committed-burst-size*: Committed burst size, number of bits that can be sent in each interval, in the range 1875 to 19375000. It defaults to the traffic passed at CIR in 500 milliseconds. If the traffic passed at CIR in 500 milliseconds is lower than 1875, 1875 is taken as the default value.

ebs *excess-burst-size*: Excessive burst size, in the range 0 to 19375000 bytes. It defaults to 0.

green: Action conducted to packets when traffic of packets conforms to the CIR. By default, the action of **green** is **pass**.

red: Action conducted to packets when traffic of packets does not conform to the CIR. By default, the action of **red** is **discard**.

action: Action conducted on a packet, which is divided into the following types:

discard: Drops the packet.

pass: Transmits the packet.

remark-dscp-pass *new-dscp*: Sets new-dscp and transmits the packet, in he range 0 to 63. When it is displayed in characters, its value can be **af11, af12, af13, af21, af22, af23, af31, af32, af33, af41, af42, af43, cs1, cs2, cs3, cs4, cs5, cs6, cs7, default, ef.**

remark-prec-pass *new-precedence*: Sets new-precedence of IP and transmits the packet, in he range 0 to 7.

Description Use the **car** command to configure traffic monitoring for a traffic behavior.

Use the **undo car** command to delete the configuration of traffic monitoring.

The policy can be used in the input or outbound direction of the interface.

Application of policy including of TP policy on an interface will cause the previous **qos car** command ineffective.

If this command is frequently configured on classes of the same policy, the last configuration will overwrite the previous ones.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Use traffic monitor for a behavior. The normal traffic of packets is 200 kbps. Burst traffic twice of the normal traffic can pass initially and later the traffic is transmitted normally when the rate does not exceed 200 kbps. When the rate exceeds 200 kbps, the IP precedence of the packet turns to 0 and the packet is transmitted.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] car cir 200 cbs 50000 ebs 0 green pass r
ed remark-prec-pass 0
```

display traffic behavior

Syntax **display traffic behavior** { **system-defined** | **user-defined** } [*behavior-name*]

View Any view

Parameters **system-defined**: Behavior pre-defined by the system.

user-defined: Behavior pre-defined by the user.

behavior-name: Behavior name. If it is not specified, the information of the behaviors pre-defined by the system or by the user will be displayed.

Description Use the **display traffic behavior** command to display the information of the traffic behavior configured on the router.

Examples # Display information about user-defined traffic behavior.

```
<Sysname> display traffic behavior user-defined
User Defined Behavior Information:
  Behavior: test
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
      Queue Length  : 64 (Packets)
    General Traffic Shape:
      CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
```

```
    Queue length 50 (Packets)
  Marking:
    Remark MPLS EXP 3
Behavior: USER1
  Marking:
    Remark IP Precedence 3
  Committed Access Rate:
    CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
    Conform Action: pass
    Exceed  Action: discard
  Expedited Forwarding:
    Bandwidth 50 (Kbps) CBS 1500 (Bytes)
```

Table 478 Description on the fields of display traffic behavior user-defined

Field	Description
User Defined Behavior Information	Behavior type: user-defined
Behavior	Behavior name and content: including multiple types
Assured Forwarding	AF information
General Traffic Shape	GTS information
Marking	Re-marking information
Committed Access Rate	CAR information
Expedited Forwarding	EF information

filter

Syntax **filter** { **deny** | **permit** }

undo filter

View Traffic behavior view

Parameters **deny**: Discards the packet.

permit: Transmits the packet.

Description Use the **filter** command to configure filter behavior for traffic behaviors.

Use the **undo filter** command to delete the configuration.

Examples # Configure the action of filtering discarded packets for traffic behavior.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] filter deny
```

gts

Syntax **gts cir** *committed-information-rate* [**cbs** *committed-burst-size* [**ebs** *excess-burst-size* [**queue-length** *queue-length*]]]

undo gts

View Traffic behavior view

Parameters **cir** *committed-information-rate*: CIR, in the range 8 to 1000000 kbps.

cbs *committed-burst-size*: CBS, in the range 1875 to 19375000 bytes, with the default value being the traffic passed at CIR in 500 milliseconds. If the traffic passed at CIR in 500 milliseconds is lower than 1875, 1875 is taken as the default value.

ebs *excess-burst-size*: EBS, in the range 0 to 19375000 bytes.

queue-length *queue-length*: The maximum length of a queue, in the range 1 to 1024. It is 50 by default.

Description Use the **gts** command to configure traffic shaping for a behavior.

Use the **undo gts** command to delete traffic shaping for a behavior.

A policy in which shape is used on an interface can only be applied in the outbound direction of the interface.

Application of class-based GTS policy including shape policy on an interface will cause the previously configured **qos gts** command ineffective.

If this command is frequently configured on the same traffic behavior, the last configuration will overwrite the previous ones.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

IPv6 is not supported for traffic shaping for software forwarding.

Examples # Configure GTS for a behavior. The normal traffic is 200 kbps. Burst traffic twice of the normal traffic can pass initially and later the traffic is transmitted normally when the rate is less than or equal to 200 kbps. When the rate exceeds 200 kbps, the traffic will enter the queue buffer and the buffer queue length is 100.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] gts cir 200 cbs 50000 ebs 0 queue-length 100
```

redirect

Syntax **redirect** { **cpu** | **interface** *interface-type interface-number* }

undo redirect

View Traffic behavior view

Parameters **cpu**: Redirects to CPU.

interface: Redirects to specified interface.

next-hop: Redirects to the next hop.

interface-type interface-number: Specifies an interface by its type and number.

Description User the **redirect** command to configure redirect action for traffic behavior.

User the **undo redirect** command to delete the configuration.

CAUTION: *When redirect action for QoS is configured, if the outbound interface to be redirected to is bound with an NAT virtual interface, packets sent from this outbound interface will be redirected to the L3+NAT card, resulting in QoS redirection failure.*

Examples # Configure redirect action for traffic behavior, to the interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] redirect interface ethernet1/0
```

remark atm-clp

Syntax **remark atm-clp** *atm-clp-value*

undo remark atm-clp

View Traffic behavior view

Parameters *atm-clp-value*: Value of the cell loss priority (CLP) bit in ATM cells, 0 or 1.

Description Use the **remark atm-clp** command to have the system remark the CLP bit of ATM cells in the class.

Use the **undo remark atm-clp** command to disable remarking the CLP bit of ATM cells.

By default, the CLP bit of ATM cells is not remarked.

The policy that includes CLP remark can apply only on the outbound direction of interfaces or ATM PVCs.

Examples # Remark the CLP bit of ATM cells to 1.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark atm-clp 1
```

remark dot1p

Syntax **remark dot1p** *8021p*

undo remark dot1p

View Traffic behavior view

Parameters *8021p*: Remarked 802.1p priority value, in the range 0 to 7.

Description Use the **remark dot1p** command to configure the 802.1p priority value of the remarked packet.

Use the **undo remark dot1p** command to remove the 802.1p priority value from the remarked packet.

By default, no 802.1p priority is marked.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Set the 802.1p priority value of the remarked packet to 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dot1p 2
```

remark dscp

Syntax **remark dscp** *dscp-value*

undo remark dscp

View Traffic behavior view

Parameters *dscp-value*: DSCP value, in the range 0 to 63, which can be any of these keywords listed in Table 479:

Table 479 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
default	000000	0
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26

Table 479 DSCP keywords and values

Keyword	DSCP value (binary)	DSCP value (decimal)
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
ef	101110	46

Description Use the **remark dscp** command to set a remarked DSCP value for IP packets belonging to the class.

Use the **undo remark dscp** command to disable DSCP remark.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Remark the DSCP of the IP packets belonging to the class to 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark dscp 6
```

remark fr-de

Syntax **remark fr-de** *fr-de-value*

undo remark fr-de

View Traffic behavior view

Parameters *fr-de-value*: Value of the DE flag bit in the FR packet, 0 or 1.

Description Use the **remark fr-de** command to set the remarked DE bit of FR packets.

Use the **undo remark fr-de** command to remove the setting.

By default, no DE bit of FR packets is configured.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Remark the DE bit in FR packets to 1.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark fr-de 1
```

remark ip-precedence

Syntax **remark ip-precedence** *ip-precedence-value*

undo remark ip-precedence

View Traffic behavior view

Parameters *ip-precedence-value*: IP precedence value, in the range 0 to 7.

Description Use the **remark ip-precedence** command to configure IP precedence remark.

Use the **undo remark ip-precedence** command to disable IP precedence remark.

By default, no IP precedence remark is configured.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Remark the IP precedence of the remarked IP packets to 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark ip-precedence 6
```

remark mpls-exp

Syntax **remark mpls-exp** *exp-value*

undo remark mpls-exp

View Traffic behavior view

Parameters *exp-value:* EXP domain value of the marked MPLS packets, in the range 0 to 7.

Description Use the **remark mpls-exp** command to configure the EXP domain value used to mark MPLS packets.

Use the **undo remark mpls-exp** command to remove the configuration.

By default, no EXP domain value used to mark MPLS packets is configured.

Examples # Configure the EXP domain value used to mark MPLS packets to 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 2
```

remark qos-local-id

Syntax **remark qos-local-id** *local-id-value*

undo remark qos-local-id

View Traffic behavior view

Parameters *local-id-value*: Remarked QoS local ID value, in the range 1 to 4095.

Description Use the **remark qos-local-id** command to configure the qos-local-id value of remarked packet.

Use the **undo remark qos-local-id** command to delete the qos-local-id value of remarked packet.

By default, no qos-local-id value of remarked packet is configured.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure the qos-local-id value of remarked packet to 2.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark qos-local-id 2
```

traffic behavior

Syntax **traffic behavior** *behavior-name*

undo traffic behavior *behavior-name*

View System view

Parameters *behavior-name*: Behavior name, a string of characters in the range 1 to 31.

Description Use the **traffic behavior** command to define a traffic behavior and enter the behavior view.

Use the **undo traffic behavior** command to delete a traffic behavior.

behavior-name shall not be the traffic behavior pre-defined by the system. The traffic behaviors defined by the system include ef, af, and be.

Related commands: **qos policy**, **qos apply policy (interface view)**, **classifier behavior**.

Examples # Define a traffic behavior named **behavior1**.

```
<Sysname> system-view
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1]
```

110
DEFINING POLICY COMMANDS

classifier behavior

Syntax **classifier** *tcl-name* **behavior** *behavior-name*

undo classifier *tcl-name*

View Policy view

Parameters *tcl-name*: Must be the name of the defined class, a string of characters in the range 1 to 31.

behavior-name: Must be the name of the defined behavior., a string of characters in the range 1 to 31.

Description Use the **classifier behavior** command to specify the behavior for the class in the policy.

Use the **undo classifier** command to remove the application of the class in the policy.

Each class in the policy can only be associated with one behavior.

If the class and traffic behavior specified when configuring this command do not exist, the system will create an empty class and an empty traffic behavior.

The **undo** command is not used for the default class.

Related commands: **qos policy**.

Examples # Specify the behavior test for the class database in the policy **user1**.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier database behavior test
[Sysname-qospolicy-user1]
```

display qos policy

Syntax **display qos policy** { **system-defined** | **user-defined** } [*policy-name* [**classifier** *tcl-name*]]

View Any view

Parameters **system-defined**: Policy pre-defined by the system.

user-defined: Policy pre-defined by the user.

policy-name: Policy name. If it is not specified, the configuration information of all the policies pre-defined by the system or by the user will be displayed.

tcl-name: Class name in the policy.

Description Use the **display qos policy** command to display the configuration information of the specified class or all the classes and associated behaviors in the specified policy or all policies.

Examples # Display the configuration information of the specified class or all the classes and associated behaviors in the user-defined policy.

```
<Sysname> display qos policy user-defined
User Defined QoS Policy Information:
Policy: test
 Classifier: default-class
   Behavior: be
    -none-

 Classifier: USER1
   Behavior: USER1
    Marking:
      Remark IP Precedence 3
    Committed Access Rate:
      CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Conform Action: pass
      Exceed  Action: discard
    Expedited Forwarding:
      Bandwidth 50 (Kbps) CBS 1500 (Bytes)

 Classifier: database
   Behavior: database
    Assured Forwarding:
      Bandwidth 30 (Kbps)
      Discard Method: Tail
      Queue Length  : 64 (Packets)
    General Traffic Shape:
      CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Queue length 50 (Packets)
    Marking:
      Remark MPLS EXP 3
```

Table 480 Description on the fields of the display qos policy command

Field	Description
Policy	Policy name
Classifier	Class name. Multiple classes may exist in a policy, each corresponding with a behavior and multiple matching rules. For details, refer to "traffic classifier" on page 1789.

Table 480 Description on the fields of the display qos policy command

Field	Description
Behavior	The behavior in a policy that corresponds with a class. Each behavior can have multiple matching rules. For details, refer to "traffic behavior" on page 1799.

display qos policy interface

Syntax **display qos policy interface** [*interface-type interface-number*] [**inbound** | **outbound**] [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

pvc: Used for ATM interface only, i.e., policy configuration of specified PVC on specified ATM interface can be displayed.

pvc-name: PVC name.

vpi/vci: VPI/VCI value pair.

Description Use the **display qos policy interface** command to view the configuration and operating state about the policy on the specified interface, on the specified PVC on a particular ATM interface or on all interfaces and PVCs.

Examples # Display the configuration and operating state about the policy on the interface Ethernet 1/0 and PVC.

```
<Sysname> display qos policy interface Ethernet 1/0
  Interface: Ethernet1/0
  Direction: Outbound
  Policy: test
   Classifier: default-class
     Matched : 0/0 (Packets/Bytes)
     Rule(s) : if-match any
     Behavior: be
     Default Queue:
      Flow Based Weighted Fair Queuing
        Max number of hashed queues: 256
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
        Discard Method: Tail

   Classifier: USER1
     Matched : 0/0 (Packets/Bytes)
     Operator: AND
     Rule(s) : if-match ip-precedence 5
     Behavior: USER1
      Marking:
        Remark IP Precedence 3
        Remarked: 0 (Packets)
```

```
    Committed Access Rate:
      CIR 200 (kbps), CBS 15000 (byte), EBS 0 (byte)
      Conform Action: pass
      Exceed  Action: discard
      Conformed: 0/0 (Packets/Bytes)
      Exceeded : 0/0 (Packets/Bytes)
    Expedited Forwarding:
      Bandwidth 50 (Kbps), CBS 1500 (Bytes)
      Matched  : 0/0 (Packets/Bytes)
      Enqueued : 0/0 (Packets/Bytes)
      Discarded: 0/0 (Packets/Bytes)

Classifier: database
  Matched : 0/0 (Packets/Bytes)
  Operator: AND
  Rule(s) : if-match acl 3131
            if-match inbound interface Ethernet1/0
  Behavior: database
   General Traffic Shape:
     CIR 300 (kbps), CBS 15000 (byte), EBS 0 (byte)
     Queue Length: 50 (Packets)
     Queue size  : 0 (Packets)
     Passed   :  0/0 (Packets/Bytes)
     Discarded:  0/0 (Packets/Bytes)
     Delayed  :  0/0 (Packets/Bytes)
   Marking:
     Remark MPLS EXP 3
     Remarked: 0 (Packets)
   Assured Forwarding:
     Bandwidth 30 (Kbps)
     Matched  : 0/0 (Packets/Bytes)
     Enqueued : 0/0 (Packets/Bytes)
     Discarded: 0/0 (Packets/Bytes)
```

Table 481 Description on the fields of the display qos policy interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Direction	Specifies the direction that the policy is applied to the interface.
Policy	Name of the policy applied to the interface
Classifier	Classification rules and corresponding configurations in the policy
Matched	Number of packets matching classification rules
Operator	Logical relationship of the classification rules in the same class
Rule(s)	Classification rules of class
Behavior	Name and configuration information of the behavior. Refer to "traffic behavior" on page 1799.

qos apply policy (interface view)

Syntax **qos apply policy** *policy-name* { **inbound** | **outbound** [**dynamic**] }

undo qos apply policy { **inbound** | **outbound** }

View Interface view

Parameters **inbound**: Inbound direction.

outbound: Outbound direction.

policy-name: Policy name, a string of characters in the range 1 to 31.

dynamic: If this argument is applied when CBQ is applied on an interface, the CBQ bandwidth will be dynamically changed with the change of the interface bandwidth.

Description Use the **qos apply policy** command to apply associated policy to the interface.

Use the **undo qos apply policy** command to delete the associated policy from the interface.

To successfully apply the policy to the interface, you must make sure that the sum of bandwidth specified for the AF and EF classes in the policy is smaller than the available bandwidth of the interface. You can modify the available bandwidth of the current interface. If the sum of their bandwidth still exceeds that modified value, the policy will be deleted.

For a policy to be applied in the inbound direction, it cannot contain classes associated with traffic behaviors specified using **queue af**, **queue ef**, **queue wfq**, or **gts**.

Applying the policy on interface following these rules:

- The VT interface referenced by common physical port and MP can apply the policy configured with various features, including **remark**, **car**, **gts**, **queue af**, **queue ef**, **queue wfq**, **wred**, etc.
- The policy configured with TS (e.g. **gts**) and queue (e.g. **queue ef**, **queue af**, **queue wfq**) features cannot be applied on the inbound interface as the input direction policy.
- Only the outbound direction policy configured with queue (e.g. **queue ef**, **queue af**, **queue wfq**) features can be applied on ATM PVC.
- The subinterface does not support queue (e.g. **queue ef**, **queue af**, **queue wfq**) features but support TS (e.g. **gts**) and TP (e.g. **car**). Therefore, the policy configured with TS and TP can be applied on the sub-interface.

Examples # Apply the policy USER1 in the outbound direction of interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos apply policy USER1 outbound
```

qos apply policy (layer 2 interface view or port group view)

Syntax **qos apply policy** *policy-name* **inbound**

undo qos apply policy { **inbound** | **outbound** }

View Layer 2 interface view/port group view

Parameters **inbound**: Inbound direction.

policy *policy-name*: Policy name, a string of characters in the range 1 to 31.

Description Use the **qos apply policy** command to apply associated policy to the interface.

Use the **undo qos apply policy** command to delete the associated policy from the interface.

The command is valid when the number of the interfaces on a layer 2 module is 16, 24 or 48.

Execute the command in interface view, and the setting is valid on the current interface only; execute the command in port group view, and the setting is valid on all ports in the port group.

Examples # Apply the policy USER1 in the inbound direction of interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos apply policy USER1 inbound
```

qos policy

Syntax **qos policy** *policy-name*

undo qos policy *policy-name*

View System view

Parameters **policy** *policy-name*: Policy name, a string of characters in the range 1 to 31.

Description Use the **qos policy** command to define a policy and enter policy view.

Use the **undo qos policy** command to delete a policy.

The policy cannot be deleted if it is applied on an interface. It is necessary to remove application of the policy on the current interface before deleting it via the **undo qos policy** command.

policy-name should not be the policy defined by the system. The "default" is the policy defined by the system.

Related commands: **classifier behavior**, **qos apply policy (interface view)**.

Examples # Define a policy named as USER1.

```
<Sysname> system-view
[Sysname] qos policy user1
[Sysname-qospolicy-user1]
```

111 FIFO QUEUING CONFIGURATION COMMANDS

qos fifo queue-length

Syntax **qos fifo queue-length** *queue-length*

undo qos fifo queue-length

View Interface view

Parameters *queue-length*: Length limit of a queue, in the range 1 to 1024. By default, the length is 75.

Description Use the **qos fifo queue-length** command to set the length limit of FIFO queue.

Use the **undo qos fifo queue-length** command to restore the default value of the queue length.

Examples # Set the length of FIFO queue to 100.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos fifo queue-length 100
```

112
PQ CONFIGURATION COMMANDS

display qos pq interface

Syntax **display qos pq interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos pq interface** command to view the configuration and statistics of priority queues (PQ) of an interface or all interfaces.

If no interfaces are specified when this command is used, the configuration and statistics of the priority queues at all interfaces will be displayed.

Related commands: **qos pq**.

Examples # Display the PQ configuration and statistics at interface Ethernet 1/0.

```
<Sysname> display qos pq interface ethernet 1/0
Interface: Ethernet1/0
Priority queueing: PQL 1  (Outbound queue:Size/Length/Discards)
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

Table 482 Description on the fields of the display pq interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Priority queuing	Priority queuing, indicating which priority queuing list will be used
Outbound queue	Outbound queue information
Size	Size of packets in the queue
Length	Queue length
Discards	The number of discarded packets

display qos pql

Syntax **display qos pql** [*pql-number*]

View Any view

Parameters *pql-number*: Priority queue list number.

Description Use the **display qos pql** command to view contents of specified PQ list (PQL) or all PQ lists.

Default items are not displayed.

Related commands: **qos pq**, **qos pq pql**.

Examples # Display PQLs.

```
<Sysname> display qos pql
Current PQL Configuration:
List  Queue   Params
-------------------------------------------------------
1     Top     Protocol ip less-than 1000
2     Normal  Length 60
2     Bottom  Length 40
3     Middle  Inbound-interface Ethernet1/0
```

qos pq

Syntax **qos pq pql** *pql-index*

undo qos pq

View Interface view

Parameters **pql**: Uses the parameters defined in specified PQ list.

pql-index: PQL index, in the range 1 to 16.

Description Use the **qos pq** command to apply a group of priority list to an interface.

Use the **undo qos pq** command to restore the congestion management policy at the interface to FIFO.

By default, the congestion management policy at the interfaces is FIFO.

Except for interfaces encapsulated with X.25, all physical interfaces can use PQ.

An interface can only use one group of priority lists.

This command can configure multiple classification rules for each group in the priority list. During traffic classification, the system matches packets along the rule list. If matching a certain rule, a packet will be classified into the priority queue specified by this rule; or it will be put into the default priority queue.

Related commands: **qos pql inbound-interface**, **display qos pq interface**, **display qos pql**, **display qos policy interface**.

Examples # Apply the priority list 12 to the Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos pq pql 12
```

qos pql default-queue

Syntax **qos pql** *pql-index* **default-queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **default-queue**

View System view

Parameters *pql-index*: PQL index, in the range 1 to 16.

top, **middle**, **normal** and **bottom**: Corresponds to the four levels of priority queue, in descending order. The queue defaults to **normal**.

Description Use the **qos pql default-queue** command to designate the packets without corresponding rules to a default queue.

Use the **undo qos pql default-queue** command to cancel the configuration and restore the default value.

During traffic classification, if a packet does not match any rule, it will be put into the default priority queue.

For the same *pql-index,* repeated use of this command will set new default queue.

Related commands: **qos pql inbound-interface**, **qos pql protocol**, **qos pql queue**, **qos pq**.

Examples # Set the default queue of the packets matching no rules in PQL 12 to be the bottom queue.

```
<Sysname> system-view
[Sysname] qos pql 12 default-queue bottom
```

qos pql inbound-interface

Syntax **qos pql** *pql-index* **inbound-interface** *interface-type interface-number* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **inbound-interface** *interface-type interface-number*

View System view

Parameters *pql-index*: PQL index, in the range 1 to 16.

interface-type interface-number: Specifies an interface by its type and number.

top, **middle**, **normal** and **bottom**: Corresponds to the four levels of priority queues, in descending order.

Description Use the **qos pql inbound-interface** command to establish classification rules based on interfaces.

Use the **undo qos pql inbound-interface** command to delete the corresponding classification rule.

By default, no classification rule is configured.

This command can match packets according to which interface the packet comes from. For the same *pql-index*, this command can be repeatedly used, establishing classification rules for packets that come from different interfaces.

Related commands: **qos pql default-queue**, **qos pql protocol**, **qos pql queue**, **qos pq**.

Examples # Create rule 12, making packets from interface serial 2/0 to be put into the middle queue.

```
<Sysname> system-view
[Sysname] qos pql 12 inbound-interface serial2/0 middle
```

qos pql protocol

Syntax **qos pql** *pql-index* **protocol ip** *queue-key key-value* **queue** { **bottom** | **middle** | **normal** | **top** }

undo qos pql *pql-index* **protocol ip** [*queue-key key-value*]

View System view

Parameters *pql-index*: PQL index, in the range 1 to 16.

top, **middle**, **normal**, **bottom**: Priority queues, in descending order.

ip: Protocol name is IP.

queue-key: Associated key of a queue.

key-value: Matching rule of a queue associated key.

When the *protocol-name* is IP, the values of *queue-key* and *key-value* are displayed in the following table:

Table 483 Description on values of queue-key and key-value

queue-key	key-value	Description
acl	*access-list-number*, 2000 to 3999	All IP packets that match the specified ACL are enqueued.
fragments	Null	All fragmented IP packets are enqueued.

Table 483 Description on values of queue-key and key-value

queue-key	key-value	Description
greater-than	Length, 0 to 65535	Any link layer frame greater than the specified value is enqueued.
less-than	Length, 0 to 65535	Link layer frames greater than the specified value are enqueued.
tcp	Port number, 0 to 65535	Any IP packet whose source or destination TCP port number is the specified port number will be classified.
udp	Port number, 0 to 65535	Any IP packet whose source or destination UDP port number is the specified port number will be classified.
--	--	All IP packets are enqueued.

When *queue-key* is tcp or udp, *key-value* can be port name or the associated port number.

Description Use the **qos pql protocol** command to establish classification rules based on the protocol type.

Use the **undo qos pql protocol** command to delete the corresponding classification rule.

By default, no rule is set.

The system matches a packet to a rule according to the set order. When the packet matches a certain rule, the search process is completed.

For the same *pql-index*, this command can be repeatedly used, establishing multiple classification rules for IP packets.

Related commands: **qos pql default-queue**, **qos pql inbound-interface**, **qos pql queue**, **qos pq**.

Examples # Specify PQ group number to 1 to make IP packets matching ACL 3100 be put into the top queue.

```
<Sysname> system-view
[Sysname] qos pql 1 protocol ip acl 3100 queue top
```

qos pql queue

Syntax **qos pql** *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length** *queue-length*

undo qos pql *pql-index* **queue** { **bottom** | **middle** | **normal** | **top** } **queue-length**

View System view

Parameters *pql-index*: PQL index, in the range 1 to 16.

queue-length: Four length values of priority queues, in the range 1 to 1024.

By default, the length values of the queues are as follows:

The default length value of the top queue is 20.

The default length value of the middle queue is 40.

The default length value of the normal queue is 60.

The default length value of the bottom queue is 80.

Description Use the **qos pql queue** command to specify the maximum number of packets that can wait in each of the priority queues, or the length of a PQ.

Use the **undo qos pql queue** command to restore to the default value of each PQ length.

If a queue is full, any newly incoming packet will be dropped.

Related commands: **qos pql default-queue**, **qos pql inbound-interface**, **qos pql protocol**, **qos pq**.

Examples # Specify the maximum number of packets waiting in the top priority queue 10 to 10.

```
<Sysname> system-view
[Sysname] qos pql 10 queue top queue-length 10
```

113
CQ CONFIGURATION COMMANDS

display qos cq interface

Syntax **display qos cq interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number: Specifies an interface by its type and number.*

Description Use the **display qos cq interface** command to view configuration and statistics of customized queues (CQ) at interfaces.

If no interface is specified, CQ configuration and statistics of all interfaces will be displayed.

Related commands: **qos cq**.

Examples # Display CQ configuration and statistics at the interface Ethernet 1/0.

```
<Sysname> display qos cq interface 1/0
Interface: Ethernet1/0
Custom queueing: CQL 1  (Outbound queue:Size/Length/Discards)
 0:   0/  20/0            1:   0/  20/0            2:   0/  20/0
 3:   0/  20/0            4:   0/  20/0            5:   0/  20/0
 6:   0/  20/0            7:   0/  20/0            8:   0/  20/0
 9:   0/  20/0           10:   0/  20/0           11:   0/  20/0
12:   0/  20/0           13:   0/  20/0           14:   0/  20/0
15:   0/  20/0           16:   0/  20/0
```

display qos cql

Syntax **display qos cql**

View Any view

Parameters None

Description Use the **display qos cql** command to view contents of customized queue lists (CPL).

Default values will not be displayed.

Related commands: **qos cq**, **qos cql default-queue**, **qos cql inbound-interface**, **qos cql protocol**, **qos cql queue**, **qos cql queue serving**.

Examples # Display information about a CQL.

```
<Sysname> display qos cql
Current CQL Configuration:
List  Queue  Params
2     3      Protocol ip fragments
3     0      Length 100
3     1      Inbound-interface Ethernet0
```

qos cq

Syntax **qos cq cql** *cql-index*

undo qos cq

View Interface view

Parameters *cql-index*: CQL index, in the range 1 to 16.

Description Use the **qos cq** command to apply the customized queue to an interface.

Use the **undo qos cq** command to restore the congestion management policy at the interface to FIFO.

By default, the congestion management policy at the interfaces is FIFO.

Except for interfaces encapsulated with X.25, all physical interfaces can use CQ.

One interface can only use one group of customized queues.

This command can configure multiple classification rules for each group in the CQL. During traffic classification, the system matches packets along the rule link. If matching a certain rule, a packet will be classified into the corresponding priority queue specified by this rule. If not matching any rule, it will go to the default priority queue.

Related commands: **qos cql default-queue**, **qos cql inbound-interface**, **qos cql protocol**, **qos cql queue serving**, **qos cql queue queue-length**.

Examples # Apply the CQ 5 on the Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos cq cql 5
```

qos cql default-queue

Syntax **qos cql** *cql-index* **default-queue** *queue-number*

undo qos cql *cql-index* **default-queue**

View System view

Parameters *cql-index*: CQL index, in the range 1 to 16.

queue-number: Queue number, in the range 0 to 16. By default, customized queue number is 1.

Description Use the **qos cql default-queue** command to assign a default queue for those packets that do not match any rule in the CQL.

Use the **undo qos cql default-queue** command to restore to the default queue.

During traffic classification, if a packet does not match any rule, it will go to the default queue.

Related commands: **qos cql inbound-interface**, **qos cql protocol**, **qos cql queue serving**, **qos cql queue**, **qos cq**.

Examples # Assign default queue 2 to CQL 5.

```
<Sysname> system-view
[Sysname] qos cql 5 default-queue 2
```

qos cql inbound-interface

Syntax **qos cql** *cql-index* **inbound-interface** *interface-type interface-number* **queue** *queue-number*

undo qos cql *cql-index* **inbound-interface** *interface-type interface-number*

View System view

Parameters *cql-index*: CQL index, in the range 1 to 16.

interface-type interface-number: Specifies an interface by its type and number.

queue-number: Queue number in the range 0 to 16.

Description Use the **qos cql inbound-interface** command to establish classification rules based on interfaces.

Use the **undo qos cql inbound-interface** command to delete corresponding classification rules.

By default, no classification rules are configured.

This command matches a packet to a rule according to the interface that the packet comes from. For the same *cql-index,* this command can be repeatedly used, establishing different classification rules for packets from different interfaces.

Related commands: **qos cql default-queue**, **qos cql protocol**, **qos cql queue serving**, **qos cql queue queue-length**

Examples # Specify a rule to put packets from the interface Ethernet 5/0 in queue 3.

```
<Sysname> system-view
[Sysname] qos cql 5 inbound-interface ethernet 5/0 queue 3
```

qos cql protocol

Syntax **qos cql** *cql-index* **protocol ip** *queue-key key-value* **queue** *queue-number*

undo qos cql *cql-index* **protocol ip** [*queue-key key-value*]

View System view

Parameters *cql-index*: CQL index, in the range 1 to 16.

queue-number: *Q*ueue number, in the range 0 to 16.

ip: Protocol name is IP.

queue-key: Associated key of a queue.

key-value: Matching rule of a queue associated key.

When *protocol-name* is IP, the values of *queue-key* and *key-value* are displayed in the following table:

Table 484 Descriptions of values of queue-key and key-value

queue-key	key-value	Description
acl	*access-list-number*, 2000 to 3999	All IP packets that match the specified ACL are enqueued.
fragments	Null	All fragmented IP packets are enqueued.
greater-than	Length, 0 to 65535	Any link layer frame greater than the specified value is enqueued.
less-than	Length, 0 to 65535	Link layer frames greater than the specified value are enqueued.
tcp	Port number, 0 to 65535	Any IP packet whose source or destination TCP port number is the specified port number will be classified.

Table 484 Descriptions of values of queue-key and key-value

queue-key	key-value	Description
udp	Port number, 0 to 65535	Any IP packet whose source or destination UDP port number is the specified port number will be classified.
--	--	All IP packets are enqueued.

When *queue-key* is tcp or udp, *key-value* can be port name or the associated port number.

Description Use the **qos cql protocol** command to establish classification rules based on the protocol type.

Use the **undo qos cql protocol** command to delete corresponding classification rules.

The system matches a packet to a rule according to the order that rules are configured. When the packet matches a certain rule, the search process is completed.

For the same *cql-index*, this command can be repeatedly used, establishing multiple classification rules for IP packets.

Related commands: **qos cql default-queue**, **qos cql inbound-interface**, **qos cql queue**, **qos cql protocol**, **qos cql queue serving**.

Examples # Specify CQ rule 5 to make any IP packet that matches the ACL 3100 be put into queue 3.

```
<Sysname> system-view
[Sysname] qos cql 5 protocol ip acl 3100 queue 3
```

qos cql queue

Syntax **qos cql** *cql-index* **queue** *queue-number* **queue-length** *queue-length*

undo qos cql *cql-index* **queue** *queue-number* **queue-length**

View System view

Parameters *cql-index*: CQL index, in the range 1 to 16.

queue-number: *Q*ueue number, in the range 0 to 16.

queue-length: The maximum length of the queue, in the range 0 to 1024. The default value is 20.

Description Use the **qos cql queue** command to configure the length of a queue, namely, the number of packets a queue can hold.

Use the **undo qos cql queue** command to restore the default.

If a queue is full, any newly incoming packet will be dropped.

Related commands: **qos cql default-queue**, **qos cql inbound-interface**, **qos pql protocol**, **qos cql queue serving**, **qos cq**.

Examples # Specify the maximum packets in the queue 4 in CQL 5 to 40.

```
<Sysname> system-view
[Sysname] qoc cql 5 queue 4 queue-length 40
```

qos cql queue serving

Syntax **qos cql** *cql-index* **queue** *queue-number* **serving** *byte-count*

undo qos cql *cql-index* **queue** *queue-number* **serving**

View System view

Parameters *cql-index*: CQL index, in the range 1 to 16.

queue-number: *Q*ueue number, in the range 0 to 16.

byte-count: Number of bytes in packets that the given queue sends in each poll, in the range 1 to 16,777,215 bytes. The default setting is 1500 bytes.

Description Use the **qos cql queue serving** command to set the byte-count of the packets sent from a given queue in each poll.

Use the **undo qos cql queue serving** command to restore the byte-count of sent packets to the default value.

By default, *byte-count* is 1500.

Related commands: **qos cql default-queue**, **qos cql inbound-interface**, **qos pql protocol**, **qos cql queue queue-length**, **qos cq**.

Examples # Specify byte-count of queue 2 in the CQL 5 to 1400.

```
<Sysname> system-view
[Sysname] qos cql 5 queue 2 serving 1400
```

114
WFQ CONFIGURATION COMMANDS

display qos wfq interface

Syntax **display qos wfq interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos wfq interface** command to view Weighted Fair Queuing (WFQ) configuration and statistics of an interface.

If no interface is specified, the WFQ configuration and statistics of all interfaces will be displayed.

Related commands: **qos wfq**.

Examples # Display the WFQ configuration and statistics of Ethernet 1/0 interface.

```
<Sysname> display qos wfq interface ethernet 1/0
Interface: Ethernet1/0
Weighted Fair queueing:   (Outbound queue:Size/Length/Discards)
  WFQ:  0/100/0
Hashed by IP Precedence
  Hashed queues:  0/0/128 (Active/Max active/Total)
```

Table 485 Description on the fields of the display qos wfq interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Outbound queue	Outbound queue information
Size	Number of packets in the queue
Length	Queue length
Hashed by	Weight type, including IP Precedence and DSCP
Discard	The number of discarded packets.
Hashed queue	Hash queue information
Active	The number of activated hash queues
Max Active	The maximum number of activated hash queues
Total	Total number of hash queues currently configured

qos wfq

Syntax **qos wfq** [**precedence** | **dscp**] [**queue-length** *max-queue-length* [**queue-number** *total-queue-number*]]

undo qos wfq

View Interface view

Parameters **precedence**: Weight type of IP precedence.

dscp: Weight type of DSCP (DiffServ code point).

max-queue-length: Maximum queue length, or maximum number of packets in each queue. It ranges from 1 to 1024 and defaults to 64. Packets out of the range will be discarded.

total-queue-number: Sum of queues. When IP precedence applies, available numbers are 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096. When dscp applies, available numbers are 64, 128, 256, 512, 1024, 2048 and 4096. The default is 256.

Description Use the **qos wfq** command to apply WFQ to the interface or modify WFQ parameters on the interface.

Use the **undo qos wfq** command to restore the default congestion management mechanism FIFO.

Except for interfaces encapsulated with X.25, all physical interfaces can use WFQ.

When WFQ is not used on interface, use the **qos wfq** command to enable the interface to use WFQ policy and specify WFQ parameters. When WFQ is used on interface, use the **qos wfq** command to modify WFQ parameters.

The weight type is **precedence** by default if no weight type is configured,

Related commands: display interface, **display qos wfq interface**.

Examples # Apply WFQ at the Ethernet 1/0 interface, set the queue length to 100 and set the total queue number to 512.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100 queue-number 512
```

115
CBQ CONFIGURATION COMMANDS

display qos cbq interface

Syntax **display qos cbq interface** [{ *interface-type interface-number* } [**pvc** { *pvc-name* [*vpi/vci*] | *vpi/vci* }]]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

pvc: Used for ATM interface only, i.e., policy configuration of specified PVC on specified ATM interface can be displayed.

pvc-name: PVC name.

vpi/vci: VPI/VCI value pair.

Description Use the **display qos cbq interface** command to display CBQ configuration information and operating status of the specified PVC on specified ATM interface or on all interfaces.

Examples # Display CBQ configuration information and operating status of the specified PVC on specified ATM interface or on all interfaces.

```
<Sysname> display qos cbq interface
Interface: Ethernet11/0
Class Based Queuing: (Outbound queue: Total Size/Discards)
  CBQ:  0/0
  Queue Size:  0/0/0 (EF/AF/BE)
  BE Queues:   0/0/256 (Active/Max active/Total)
  AF Queues:   1 (Allocated)
  Bandwidth(Kbps): 74992/75000 (Available/Max reserve)
```

qos max-bandwidth

Syntax **qos max-bandwidth** *bandwidth*

undo qos max-bandwidth

View Interface view

Parameters *bandwidth:* Maximum bandwidth available on an interface, in the range 1 t o1000000 kbps

Description Use the **queue max-bandwidth** command to configure the maximum bandwidth available on an interface.

Use the **undo queue max-bandwidth** command to restore the default.

By default:

For a physical interface, the value is the actual baudrate or speed of the physical interface;

For logical serial interfaces such as T1/E1 and MFR created by binding the value is the sum of bandwidth on the channels they are bound to.

For logical interfaces such as Virtual Template and VE, the value is 0 kbps.

- *It is recommended that the maximum available bandwidth be smaller than the actual available bandwidth of physical interface or logical link.*
- *Modification of the maximum available bandwidth may trigger CBQ reconstruction, thus resulting in CBQ's reallocation of queue width. The modification of the baudrate or speed of a physical interface, however, does not trigger this reconstruction process.*
- *To apply QoS policies to a logical interface properly, you must use the **shutdown** command to shut down all the physical interfaces bound to the logical interface and then use the **undo shutdown** command to bring up these physical interfaces again.*

Examples # Configure the maximum bandwidth on the interface Ethernet1/0 to 16 kbps.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100
```

queue af

Syntax **queue af bandwidth** { *bandwidth* | **pct** *percentage* }

undo queue af

View Traffic behavior view

Parameters *bandwidth*: Bandwidth in kbps, in the range 8 to 1000000.

percentage: Percentage of the available bandwidth, in the range 1 to 100.

Description Use the **queue af** command to configure the class to perform AF and the minimum bandwidth used.

Use the **undo queue af** command to cancel the configuration.

When associating the class with the **queue af** behavior in the policy, the following must be satisfied.

The sum of the bandwidth specified for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must be less than or equal to the available bandwidth of the interface where the policy is applied.

The sum of percentages of the bandwidth specified for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must be less than or equal to 100.

The bandwidth configuration for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must adopt the value of the same type. For example, they all adopt the absolute value form or the percentage form.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure traffic behavior named database and configure the minimum bandwidth of the traffic behavior to 200 kbps.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
```

queue ef

Syntax **queue ef bandwidth** { *bandwidth* [**cbs** *burst*] | **pct** *percentage* [**cbs-ratio** *ratio*] }

undo queue ef

View Traffic behavior view

Parameters *bandwidth*: Bandwidth in kbps, in the range 8 to 1000000.

cbs *burst*: Specifies the committed burst size in byte, in the range 32 to 2000000, By default, *burst* is bandwidth*25.

pct *percentage*: Percentage of available bandwidth, in the range 1 to 100.

cbs-ratio *ratio*: Committed burst percentage, in the range 25 to 500. By default, the value is 25.

Description Use the **queue ef** command to configure EF packets to the absolute priority queue and configure the maximum bandwidth.

Use the **undo queue ef** command to cancel the configuration.

When configuring this command, keep the following in mind:

The command can not be used together with **queue af**, **queue-length**, and **wred** in traffic behavior view.

In the policy the default class default-class cannot be associated with the traffic behavior **queue ef** belongs to.

The sum of the bandwidth specified for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must be less than or equal to the available bandwidth of the interface where the policy is applied.

The sum of percentages of the bandwidth specified for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must be less than or equal to 100.

The bandwidth configuration for the classes in the same policy to assured forwarding (**queue af**) and expedited forwarding (**queue ef**) must adopt the value of the same type. For example, they all adopt the absolute value form or the percentage form.

For the percentage form **queue ef bandwidth pct** *percentage* [**cbs-ratio** *ratio*], CBS = Interface available bandwidth**percentage***ratio*/100/1000

For the absolute value form **queue ef bandwidth** *bandwidth* [**cbs** *burst*], CBS = burst, or = *bandwidth**25 if *burst* is not specified.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure packets to enter priority queue. The maximum bandwidth is 200 kbps and CBS is 5000 bytes.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue ef bandwidth 200 cbs 5000
```

queue wfq

Syntax **queue wfq** [**queue-number** *total-queue-number*]

undo queue wfq

View Traffic behavior view

Parameters *total-queue-number*: Number of fair queue, which can be 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096 and the default value is 64.

Description Use the **queue wfq** command to configure the default-class to use WFQ.

Use the **undo queue wfq** command to delete the configuration.

The traffic behavior configured with the command can only be associated with the default class. It can also be used together with the command like **queue-length** or **wred**.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure WFQ for default-class and the queue number is 16.

```
<Sysname> system-view
[Sysname] traffic behavior test
[Sysname-behavior-test] queue wfq 16
[Sysname] qos policy user1
[Sysname-qospolicy-user1] classifier default-class behavior test
```

queue-length

Syntax **queue-length** *queue-length*

undo queue-length *queue-length*

View Traffic behavior view

Parameters *queue-length*: The maximum threshold value of the queue, in the range 1 to 512. The queue length is 64.

Description Use the **queue-length** command to configure maximum queue length, and the drop mode is tail drop.

Use the **undo queue-length** command to delete configuration.

By default, tail drop is configured.

This command can be used only after the **queue af** or **queue wfq** command has been configured.

The **queue-length**, which has been configured, will be deleted when the **undo queue af** or **undo queue wfq** command is executed.

The **queue-length**, which has been configured, will be deleted when the random drop mode is configured via the **wred** command, and vise versa.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure tail drop and set the maximum queue length to 16.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] queue-length 16
```

wred

Syntax **wred** [**dscp** | **ip-precedence**]

undo wred

View Traffic behavior view

Parameters **dscp**: Uses DSCP value for calculating drop probability for a packet.

ip-precedence: Uses IP precedence value for calculating drop probability for a packet.

Description Use the **wred** command to configure drop mode as Weighted Random Early Detection (WRED).

Use the **undo wred** command to remove the configuration.

This command can be used only after the **queue af** or **queue wfq** command has been configured. The **wred** command and **queue-length** command can not be used simultaneously. Other configurations under the random drop will be deleted when this command is deleted. When a policy is applied on an interface, the previous WRED configuration on interface level will become ineffective.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure to adopt WRED and count discard rate with IP precedence.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred
```

wred dscp

Syntax **wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred dscp *dscp-value*

View Traffic behavior view

Parameters *dscp-value*: DSCP value, in the range 0 to 63, which can also be any of the keywords listed in Table 479.

low-limit *low-limit*: Specifies the lower threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 10.

high-limit *high-limit*: Specifies the upper threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 30.

discard-probability *discard-prob*: Specifies the denominator for drop probability, in the range 1 to 255. The system default is 10.

Description Use the **wred dscp** command to set DSCP lower-limit, upper-limit and drop probability denominator of WRED.

Use the **undo wred dscp** command to delete the configuration.

This command can be used only after the **wred** command has been used to enable WRED drop mode based on DSCP.

The configuration of **wred dscp** will be deleted if the configuration of **qos wred** is deleted.

The configuration of drop parameter gets invalid if the configuration of the **queue af** command or the **queue wfq** command is cancelled.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Set the queue lower-limit to 20, upper-limit to 40 and discard probability to 15 for the packet whose DSCP is 3.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred dscp
[Sysname-behavior-database] wred dscp 3 low-limit 20 high-limit 40 d
iscard-probability 15
```

wred ip-precedence

Syntax **wred ip-precedence** *precedence* **low-limit** *low-limit* **high-limit** *high-limit* [**discard-probability** *discard-prob*]

undo wred ip-precedence *precedence*

View Traffic behavior view

Parameters *precedence*: IP precedence, in the range 0 to 7.

low-limit *low-limit*: Specifies the lower threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 10.

high-limit *high-limit*: Specifies the upper threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 30.

discard-probability *discard-prob*: Specifies the denominator for drop probability, in the range 1 to 255. The system default is 10.

Description Use the **wred ip-precedence** command to set precedence lower-limit, upper-limit and drop probability denominator of WRED.

Use the **undo wred ip-precedence** command to delete the configuration.

The **wred ip-precedence** command can be used only after the **wred** command is used to enable IP precedence-based WRED drop mode.

The configuration of **wred ip-precedence** will be deleted when **wred** configuration is deleted.

The configuration of drop parameters gets invalid if the configuration of the **queue af** command or the **queue wfq** command is cancelled.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Set lower-limit to 20, upper-limit to 40 and discard probability to 15 for the packet with the precedence 3.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue wfq
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred ip-precedence 3 low-limit 20 high-l
imit 40 discard-probability 15
```

wred weighting-constant

Syntax **wred weighting-constant** *exponent*

undo wred weighting-constant

View Traffic behavior view

Parameters *exponent*: Exponential, in the range 1 to 16. It is 9 by default.

Description Use the **wred weighting-constant** command to set exponential for the calculation of average queue length by WRED.

Use the **undo wred weighting-constant** command to delete the configuration.

This command can be used only after the **queue af** command or the **queue wfq** command has been configured and the **wred** command has been used to enable WRED drop mode.

The configuration of **wred weighting-constant** will be deleted if **wred** is deleted.

Related commands: **qos policy**, **traffic behavior**, **classifier behavior**.

Examples # Configure exponential for calculating average queue length to 6.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] queue af bandwidth 200
[Sysname-behavior-database] wred ip-precedence
[Sysname-behavior-database] wred weighting-constant 6
```

116
RTP PRIORITY QUEUE CONFIGURATION COMMANDS

display qos rtpq interface

Syntax **display qos rtpq interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display qos rtpq interface** command to view information of the current IP RTP Priority queue, including the current RTP queue depth and number of RTP packets dropped.

If no interface is specified, it will display the RTP priority queue configuration and statistics on all interfaces.

Examples # Display information of the current IP RTP Priority queue.

```
<Sysname> display qos rtpq interface
Interface: Ethernet1/0
Output queue : (RTP queue : Size/Max/Outputs/Discards)  0/0/0/0
```

Table 486 Description on the fields of the display qos rtpq command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Output queue	Current output queue
Size	Number of packets in the queue
Max	Maximum number of packets the queue ever holds
Outputs	Number of transmitted packets
Discards	Number of discarded packets

qos reserved-bandwidth

Syntax **qos reserved-bandwidth pct** *percent*

undo qos reserved-bandwidth

View Interface view

Parameters **pct** *percent*: Percentage of the reserved bandwidth to the available bandwidth. It is in the range 1 to 100 and the default value is 80.

Description Use the **qos reserved-bandwidth** command to set the maximum reserved bandwidth percentage.

Use the **undo qos reserved-bandwidth** command to restore the default value.

Usually the bandwidth configured for the QoS queue is less than 80 percent of the total bandwidth, considering that part of the bandwidth should be used for controlling protocol packets, layer 2 frame headers and so on.

Caution should be taken in using this command to modify the maximum preserved bandwidth.

Related commands: **qos rtpq**.

Examples # Set the maximum reserved bandwidth allocated for RTP priority queue to 70% of the available bandwidth.

```
<Sysname> system-view
[Sysname] interface Serial1/0
[Sysname-Serial1/0] qos reserved-bandwidth pct 70
```

qos rtpq

Syntax **qos rtpq start-port** *first-rtp-port-numbe*r **end-port** *last-rtp-port-number* **bandwidth** *bandwidth* [**cbs** *burst*]

undo qos rtpq

View Interface view

Parameters **start-port** *first-rtp-port-number*: Specifies the first UDP port number to initiate RTP messages, in the range 2000 to 65535.

end-port *last-rtp-port-number*: Specifies the last UDP port number to initiate RTP messages, in the range 2000 to 65535.

bandwidth *bandwidth*: Bandwidth for RTP priority queue, which is part of the maximum reserved bandwidth in kbps, in the range 8 to 1000000.

cbs *burst*: Committed burst size, in the range 1500 to 2000000 in byte.

Description Use the **qos rtpq** command to enable RTP queue feature on an interface so as to reserve a real-time service for the RTP packets sent to some UDP destination port ranges.

Use the **undo qos rtpq** command to disable the RTP queuing feature of the interface.

By default, RTP queuing feature is disabled.

This command is applied to the delay-sensitive applications, real-time voice transmission for example. Configured with the **qos rtpq** command, the system will serve the voice services first among all other services.

The parameter *bandwidth* should be set greater than the service-required bandwidth so as to prevent conflict caused by the burst traffic.

However, the bandwidth should be no greater than 80% of the total bandwidth. If you need to configure the bandwidth to be greater than 80% of the total bandwidth, please first change the maximum reserved bandwidth via **qos reserved-bandwidth** command.

In bandwidth allocation, the bandwidth for data load, IP header, UDP header and RTP header is allocated, except that for the Layer 2 frame header. Therefore, it is obligatory to reserve 20% of the total bandwidth.

Related commands: **qos reserved-bandwidth**.

Examples # Enable RTP priority queue feature on Serial 1/0. The starting UDP port number is 16384. The end UDP port number is 32767. The RTP packets use 64 kbps bandwidth. If network convergence happens, the packets will enter RTP priority queue.

```
<Sysname> system-view
[Sysname] interface Serial1/0
[Sysname-serial1/0] qos rtpq start-port 16384 end-port 32767 bandwidth 64
```

117 QoS Token Configuration Commands

qos qmtoken

Syntax **qos qmtoken** *token-number*

undo qos qmtoken

View Interface view

Parameters *token-number*: The number of transmitted tokens, in the range 1 to 50.

Description Use the **qos qmtoken** command to configure the number of transmitted tokens.

Use the **undo qos qmtoken** command to disable the token transmission function of QoS.

By default, the function of QoS is disabled.

During an FTP transfer, flow control provided by the upper layer protocol can invalidate the configuration of QoS queuing. To resolve this problem, the token transmission function of QoS was introduced. This function provides a flow control mechanism at the underlying-layer queuing level. It can control the number of packets sent to the underlying interface queues based on the number of tokens.

If FTP applies, you are recommended to set the number of tokens sent by an interface to 1.

- *After you configure this command on an interface, you must perform **shutdown** and **undo shutdown** on the interface to have the function take effect.*
- *So far, this command is supported only by Ethernet, serial, and BRI interfaces.*

Examples # Set the number of transmitted tokens to 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] qos qmtoken 1
```

118
PRIORITY MAPPING TABLE CONFIGURATION COMMANDS

display qos map-table

Syntax **display qos map-table** [**dot1p-lp**]

View Any view

Parameters **dot1p-lp**: Mapping table of 802.1p priority to local priority.

Description Use the **display qos map-table** command to display configuration of specified priority mapping table

If the type of table is not specified, the configuration information of all mapping tables will be displayed.

Related commands: **qos map-table dot1p-lp**.

Examples # Display configuration information about the mapping table of 802.1p priority to local priority.

```
<Sysname> display qos map-table dot1p-dp
MAP-TABLE NAME: dot1p-lp   TYPE: pre-define
IMPORT  :  EXPORT
   0    :    2
   1    :    0
   2    :    1
   3    :    3
   4    :    4
   5    :    5
   6    :    6
   7    :    7
```

Table 487 Description on the fields of the display qos map-table command

Field	Description
MAP-TABLE NAME	Name of the mapping table
TYPE	Type of the mapping table
IMPORT	Import entry of the mapping table
EXPORT	Export entry of the mapping table

qos map-table dot1p-lp

Syntax **qos map-table dot1p-lp**

View System view

Parameters **dot1p-lp**: Mapping table of 802.1p priority to local priority.

Description Use the **qos map-table** command to enter the specified priority mapping table view.

Related commands: **display qos map-table**.

Examples # Enter the mapping table view from 802.1p priority to local priority.

```
<Sysname> system-view
[Sysname]qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp]
```

import

Syntax **import** *import-value-list* **export** *export-value*

undo import { *import-value-list* | **all** }

View Priority mapping table view

Parameters *import-value-list*: Maps input parameter list.

export-value: Maps export parameters.

all: Deletes all parameters in this mapping table.

Description Use the **import** command to configure the parameters in the specified priority mapping table to define a mapping rule or a group of mapping rules.

Use the **undo import** command to delete the mapping entries corresponding to specified mapping index. The deleted entries are restored to default value.

The default value is shown in the following table:

Table 488 Parameters in the default mapping table

802.1p priority	Local priority
0	2
1	0
2	1
3	3

Table 488 Parameters in the default mapping table

802.1p priority	Local priority
4	4
5	5
6	6
7	7

Related commands: **display qos map-table**.

Examples # Configure the parameters in the mapping table from 802.1p priority to local priority. The local priority corresponding to 802.1p priority 4 and 5 is local priority 1.

```
<Sysname> system-view
[Sysname] qos map-table dot1p-lp
[Sysname-maptbl-dot1p-lp] import 4 5 export 1
```

119 PORT PRIORITY CONFIGURATION COMMANDS

qos priority

Syntax **qos priority** *priority-value*

undo qos priority

View Ethernet interface view/port group view

Parameters *priority-value*: Port priority value, in the range 0 to 7. The default value is 0.

Description Use the **qos priority** command to configure the port priority of current port.

Use the **undo qos priority** command to restore to the default value.

Port group is supported if the number of the interfaces on a layer 2 module is 16, 24 or 48.

Execute the command in interface view, and the setting is effective on the current interface only. Execute the command in interface group view, and the setting is effective on all interfaces in the interface group.

Examples # Configure the Ethernet 1/0 priority to 2.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] qos priority 2
```

120 PORT PRIORITY TRUST MODE CONFIGURATION COMMANDS

display qos trust interface

Syntax **display qos trust interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number:* Specifies an interface by its type and number.

Description Use the **display qos trust interface** command to display the information about the port priority trust mode currently configured.

If no interface is specified, the port priority trust mode of all interfaces will be displayed.

Examples # Display the information about the port priority trust mode currently configured.

```
<Sysname> display qos trust interface ethernet 1/0
Interface: Ethernet1/0
Port priority information
Port priority :4
```

Table 489 Description on the fields of the display qos trust interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Port priority	Port priority

qos trust

Syntax **qos trust dot1p**

undo qos trust

View L2 module Ethernet interface view/port group view

Parameters **dot1p**: Specifies to trust 802.1p priority carried with a packet, and perform priority mapping using this priority.

Description Use the **qos trust** command to set to trust 802.1p priority carried with a packet.

Use the **undo qos trust** command to restore the default.

By default, 802.1p priority carried with a packet is not trusted.

Port group is supported if the number of the interfaces on a layer 2 module is 16, 24 or 48.

Execute the command in interface view, and the setting is valid on the current interface only. Execute the command in interface group view, and the setting is valid on all interfaces in the interface group.

Examples # Configure the priority trust mode on the port Ethernet 1/0 to be 802.1p priority carried with the trust packet.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] qos trust dot1p
```

121
WRED CONFIGURATION COMMANDS

display qos wred interface

Syntax **display qos wred interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number:* Specifies an interface by its type and number.

Description Use the **display qos wred interface** command to view WRED configuration and statistics of an interface.

If no interface is specified, WRED configuration and statistics of all interfaces will be displayed.

Examples # Display WRED configuration and statistics about the specified interface.

```
<Sysname> display qos wred interface ethernet 1/0
Interface: Ethernet1/0
Current WRED configuration:
 Exponent: 9 (1/512)
 Precedence Low     High    Discard      Random      Tail
            Limit   Limit   Probability  Discard     Discard
 ------------------------------------------------------------
 0            10      30        10             0           0
 1            100     1000      1              0           0
 2            10      30        10             0           0
 3            10      30        10             0           0
 4            10      30        10             0           0
 5            10      30        10             0           0
 6            10      30        10             0           0
 7            10      30        10             0           0
```

Table 490 Description on the fields of the display qos wred interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Exponent	Exponent for calculating the average queue length
Precedence	IP precedence of packet
Random discard	Number of random-discard packets
Tail discard	Number of tail-discard packets
Low limit	Lower limit for queue

Table 490 Description on the fields of the display qos wred interface command

Field	Description
High limit	Higher limit for queue
Discard probability	Denominator for calculating drop probability

Display the WRED configuration and statistics of the specified interface.

```
<Sysname> display qos wred interface
Interface: Ethernet1/0
  Current WRED configuration:
Applied Wred table name: q1
Table Type: Queue based WRED
QID:    green-discard     yellow-discard      red-discard     total-discard
          (Packets)          (Packets)         (Packets)          (Packets)
------------------------------------------------------------------------------
0            100                      200                     300             600
1                0                        0                       0             0
2                0                        0                       0             0
3                0                        0                       0             0
4                0                        0                       0             0
5                0                        0                       0             0
6                0                        0                       0             0
7                0                        0                       0             0
```

Table 491 Description on the fields of the display qos wred interface command

Field	Description
Interface	Interface name, consisting of interface type and interface number
Applied Wred table name	WRED table name
Table Type	WRED table type
QID	Queue ID
green-discard(Packets)	Number of the green-discard packets
yellow-discard(Packets)	Number of the yellow-discard packets
red-discard(Packets)	Number of the red-discard packets
total-discard(Packets)	Number of the total-discard packets

qos wred enable

Syntax **qos wred** [**dscp** | **ip-precedence**] **enable**

undo qos wred enable

View Interface view

Parameters **dscp**: Uses the DSCP value for calculating drop probability.

ip-precedence: Uses the IP precedence value for calculating drop probability. By default, IP precedence is used for calculating drop probability.

Description Use the **qos wred enable** command to apply WRED at an interface.

Use the **undo qos wred enable** command to restore the default dropping method.

By default, the dropping method of a queue is tail drop.

Related commands: **qos wfq**, **display qos wred interface**.

Examples # Enable WRED on Ethernet 1/0, using IP precedence for calculating the drop probability.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/0] qos wred ip-precedence enable
```

qos wred dscp

Syntax **qos wred dscp** *dscp-value* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred dscp *dscp-value*

View Interface view

Parameters *dscp-value*: DSCP value, in the range of 0 to 63. This argument can also be a keyword listed in Table 479.

low-limit *low-limit*: Specifies the lower threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 10.

high-limit *high-limit*: Specifies the upper threshold, in the range 1 to 1024 (in terms of the number of packets). The system default is 30.

discard-probability *discard-prob*: Specifies the denominator for drop probability, in the range 1 to 255. The system default is 10.

Description Use the **qos wred dscp** command to set the lower threshold, the higher threshold, and drop probability denominator for a specific DSCP value.

Use the **undo qos wred dscp** command to restore the default.

Before performing this configuration, make sure that the **qos wred dscp enable** command is used to apply DSCP-based WRED to the interface. The thresholds limit the average queue length.

Related commands: **qos wred enable**, **display qos wred interface**.

Examples # Configure the following parameters for packets with the DSCP value 63: lower threshold 20, higher threshold 40, and drop probability denominator 15.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/0] qos wred dscp enable
```

```
[Sysname-Ethernet1/0] qos wred dscp 63 low-limit 20 high-limit 40 di
scard-probability 15
```

qos wred ip-precedence

Syntax **qos wred ip-precedence** *ip-precedence* **low-limit** *low-limit* **high-limit** *high-limit* **discard-probability** *discard-prob*

undo qos wred ip-precedence *ip-precedence*

View Interface view

Parameters **ip-precedence** *ip-precedence*: Specifies an IP precedence, in the range 0 to 7;

low-limit *low-limit*: Specifies the lower threshold, in the range 1 to 1024. This argument is 10 by default.

high-limit *high-limit*: Specifies the higher threshold, in the range 1 to 1024. This argument is 30 by default.

discard-probability *discard-prob*: Specifies the drop probability denominator, in the range 1 to 255. This argument is 10 by default.

Description Use the **qos wred ip-precedence** command to configure the lower threshold, the higher threshold, and the drop probability denominator for an IP precedence value.

Use the **undo qos wred ip-precedence** command to restore the default.

WRED parameters can be set only after the **qos wfq** command has been used to apply WFQ and the **qos wred enable** command has been used to apply IP precedence-based WRED to the interface. The thresholds limit the average queue length.

Related commands: **qos wfq**, **qos wred enable**, **display qos wred interface**.

Examples # Set lower threshold of the packet of precedence 3 at an interface to 20, the higher threshold to 40, and the discard probability to 15.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/0] qos wred ip-precedence enable
[Sysname-Ethernet1/0] qos wred ip-precedence 3 low-limit 20 high-lim
it 40 discard-probability 15
```

qos wred weighting-constant

Syntax **qos wred weighting-constant** *exponent*

undo qos wred weighting-constant

View Interface view

Parameters **weighting-constant** *exponent*: Exponent used to calculate the average queue length, in the range 1 to 16. It defaults to 9.

Description Use the **qos wred weighting-constant** command to set exponential used to calculate the average length of WRED queues.

Use the **undo qos wred weighting-constant** command to restore the default.

Before you can configure WRED parameters on an interface, you must apply WRED with the **qos wred enable** command on it.

Related commands: **qos wred enable**, **display qos wred interface**.

Examples # Set the exponent used to calculate average queue length to 6 on Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet1/0
[Sysname-Ethernet1/0] qos wfq queue-length 100 queue-number 512
[Sysname-Ethernet1/0] qos wred enable
[Sysname-Ethernet1/0] qos wred weighting-constant 6
```

122 WRED TABLE CONFIGURATION COMMANDS

display qos wred table

Syntax **display qos wred table** [*table-name*]

View Any view

Parameters *table-name*: Name of the WRED table to be displayed.

Description Use the **display qos wred table** command to display the configuration information of WRED table.

If no table name is specified, the configuration information of all WRED tables will be displayed.

Examples # Display configuration information of WRED table1, which is the list for configured WRED parameters.

```
<Sysname> display qos wred table 1
Table Name: 1
Table Type: EXP based WRED
Exponent: 6
Precedence    LowLimit       HighLimit       DiscardProbability
 ----------------------------------------------------------------------
 0                 0                 0              10
 1                 0                 0              10
 2                 0                 0              10
 3                 0                 0              10
 4                 0                 0              10
 5                 0                 0              10
 6                 0                 0              10
 7                 0                 0              10
```

Table 492 Description on the fields of the display qos wred table command

Field	Description
Table name	WRED table name
Table type	WRED table type
Exponent	Exponent for calculating average queue length
Precedence	Packet precedence level
Low limit	Lower limit of the queue
High limit	Higher limit of the queue

Table 492 Description on the fields of the display qos wred table command

Field	Description
Discard probability	Denominator for calculating drop probability

qos wred queue table

Syntax **qos wred queue table** *table-name*

undo qos wred table *table-name*

View System view

Parameters **queue**: Queue-based table, which randomly drops packets according to the queue the packet belongs to when congestion occurs.

table *table-name*: Specified the table name, a string of characters in the range 1 to 32.

Description Use the **qos wred queue table** command to create WRED table and enter the WRED table view.

Use the **undo qos wred table** command to delete the global WRED table.

By default, no global WRED table exists.

It is not allowed to delete the table being used.

The queue-based WRED table can be applied only on Layer 2 port, on which the queue-based WRED table can be applied only.

Related commands: **qos wfq**, **qos wred enable**, **display qos wred interface**.

Examples # Create queue-based WRED table exp-table1.

```
<Sysname> system-view
[Sysname] qos wred queue table exp-table1
[Sysname-wred-table-queue-table1]
```

qos wred apply

Syntax **qos wred apply** *table-name*

undo qos wred apply

View L2 interface view/port group view

Parameters *table-name*: Specifies the WRED table name.

Description Use the **qos wred apply** command to apply WRED table on an interface.

Use the **undo qos wred apply** command to restore the default dropping method. This command also deletes the application of WRED table.

By default, the dropping method of a queue is tail drop.

The queue-based WRED table can be applied only on a Layer 2 interface and on a layer 2 interface only the queue-based WRED table can be applied.

Execute the command in interface view, and the setting is valid on the current interface only. Execute the command in interface group view, and the setting is valid on all interfaces in the interface group.

Related commands: **display qos wred interface**, **display qos wred table**, **qos wred queue table**.

Examples # Apply queue-based WRED table queue-table1 on a layer 2 interface.

```
<Sysname> system-view
[Sysname] interface Ethernet1/0
[Sysname-Ethernet1/0] qos wred apply queue-table1
```

queue

Syntax **queue** *queue-value* **low-limit** *low-limit* [**discard-probability** *discard-prob*]

undo queue { *queue-value* | **all** }

View WRED table view

Parameters *queue-value*: Queue number, which is applicable to L2 port only. It ranges from 0 to 3.

low-limit *low-limit*: Lower threshold, in the range 1 to 128. It defaults to 10.

discard-probability *discard-prob*: Denominator of drop probability; each drop level has an independent drop probability denominator. It ranges from 1 to 16 and defaults to 10.

Description Use the **queue** command to edit the content of the queue-based WRED table.

Use the **undo queue** command to restore the content to be default value.

By default, the queue-based WRED global table has a set of usable default parameters. Therefore, there are no default values for the parameters during editing. As long as no value is specified, the default values keep unchanged.

Related commands: **qos wred queue table** (in system view).

Examples # Modify the drop parameter with a lower threshold of 10 of the packet in the queue 1 of queue-based global WRED table queue-table1.

```
<Sysname> system-view
[Sysname] qos wred queue table queue-table1
[Sysname-wred-table-queue-table1] queue 1 low-limit 10
```

123
MPLS QoS CONFIGURATION COMMANDS

if-match mpls-exp

Syntax **if-match** [**not**] **mpls-exp** *exp-value-list*

undo if-match [**not**] **mpls-exp**

View Class view

Parameters *exp-value-list*: EXP value list, in the range 0 to 7. Users can input the eight values repeatedly.

Description Use the **if-match mpls-exp** command to configure the matching rule for EXP domain of MPLS.

Use the **undo if-match mpls-exp** command to delete the matching rule.

If this command is frequently configured under one class, the last configuration will overwrite the previous ones.

Related commands: **traffic classifier**.

Examples # Define the rule to match the packet whose EXP is 3 or 4.

```
<Sysname> system-view
[Sysname] traffic classifier database
[Sysname-classifier-database] if-match mpls-exp 3 4
```

qos cql protocol mpls exp

Syntax **qos cql** *cql-index* **protocol mpls exp** *exp-value* **queue** *queue*

undo qos cql *cql-index* **protocol mpls exp** *exp-value*

View System view

Parameters *cql-index*: Group number of custom queuing list (CQL), in the range 1 to 16.

queue: Queue number of CQ, in the range 0 to 16.

exp-value: EXP domain of MPLS packet, in the range 0 to 7. Up to 8 can be configured, separated with space.

Description Use the **qos cql protocol mpls exp** command to configure CQ classification rule based on the MPLS protocol.

Use the **undo qos cql protocol mpls exp** command to delete the corresponding classification rule.

For the same *cql-index*, this command can be used repeatedly to establish multiple types of classification rules for IP packets.

When multiple rules are present, the device matches packets in the sequence that rules are configured.

Related commands: **qos cql protocol**.

Examples # Configure classification rule based on the MPLS protocol CQL 10, and sets the queue 1 to correspond with EXP value 1.

```
<Sysname> system-view
[Sysname] qos cql 10 protocol mpls exp 1 queue 1
```

qos pql protocol mpls exp

Syntax **qos pql** *pql-index* **protocol mpls exp** *exp-value* **queue** { **top** | **middle** | **normal** | **bottom** }

undo qos pql *pql-index* **protocol mpls exp** *exp-value*

View System view

Parameters *pql-index*: Group number of priority queuing list (PQL), in the range 1 to 16.

queue: Queue name, which is valued **top, middle, normal** and **bottom.**

exp-*value*: EXP domain value of MPLS packet, in the range 0 to 7. Up to 8 can be configured, separated with space.

Description Use the **qos pql protocol mpls exp** command to establish the PQL classification rule based on MPLS protocol.

Use the **undo qos pql protocol mpls exp** command to delete corresponding PQL classification rules.

For the same *pql-index*, this command can be used repeatedly to establish several types of PQL classification rules for IP packets.

When multiple rules are present, the device matches packets in the sequence that rules are configured.

Related commands: **qos pql protocol**.

Examples # Configure classification rule based on the MPLS protocol CQL 10, and sets the queue top to correspond with EXP value 5.

```
<Sysname> system-view
[Sysname] qos pql 10 protocol mpls-exp 5 queue top
```

remark mpls-exp

Syntax **remark mpls-exp** *exp-value*

undo remark mpls-exp

View Traffic behavior view

Parameters *exp-value*: EXP value of MPLS, in the range 0 to 7.

Description Use the **remark mpls-exp** command to configure the EXP value of remarked MPLS packet.

Use the **undo remark mpls-exp** command to remove the configuration.

Related commands: **traffic classifier**, **qos policy**, **classifier behavior**.

Examples # Set EXP value of remarked MPLS packet to 0.

```
<Sysname> system-view
[Sysname] traffic behavior database
[Sysname-behavior-database] remark mpls-exp 0
```

124 DAR CONFIGURATION COMMANDS

dar max-session-count

Syntax **dar max-session-count** *count*

undo dar max-session-count

View System view

Parameters *count*: The maximum number of connections recognizable by DAR, in the range 0 to 65536. It defaults to 65536.

Description Use the **dar max-session-count** command to configure the maximum number of connections recognizable by DAR.

Use the **undo dar max-session-count** command to restore the default value.

When large data volume goes through the device, it often takes too many system resources to recognize them one by one with DAR, which also impacts working of other modules. To avoid the case, users can limit the maximum number of connections that can be recognized by DAR in order to save system resources. When the connection number exceeds the maximum threshold, DAR will not recognize it and directly mark it to be unrecognizable.

Examples # Set the maximum number of connections recognizable by DAR to 1000.

```
<Sysname> system-view
[Sysname] dar max-session-count 1000
```

dar protocol

Syntax **dar protocol** *protocol-name* { **tcp** | **udp** } **port** { *port-value* | **range** *port-min port-max* } *

undo dar protocol *protocol-name* { **tcp** | **udp** } **port**

View System view

Parameters *protocol-name*: Application protocol type. As shown in Table 493, the range can be all protocols listed in the table, or Bittorrent, RTP, RTCP and ten user-defined

protocols, including **user-defined01**, **user-defined02**, ..., **user-defined10**. No port number is specified for the user-defined protocol at the initial state. It will be effective only after the port number is specified. At the same time, the **dar protocol-rename** command can be used to modify the name of user-defined protocol.

tcp: Based on TCP.

udp: Based on UDP.

port-value: Port number of protocol, in the range 1 to 65535, which cannot be the same with the configured port number of other protocols in the DAR feature. Up to 16 port numbers can be set for each protocol, which are separated with spaces.

range *port-min port-max*: Set the range of port number, *port-min* for the minimum port number, and *port-max* for the minimum port number . The difference value between the maximum number and minimum number shall be smaller than 1000, i.e. *port-max* - *port-min* < 1000. The port number of other application protocols in the DAR feature cannot be within the range.

Table 493 Protocols of pre-defined ports

Protocol name	Protocol type	Pre-defined port number
BGP	TCP/UDP	179
Citrix	TCP	1494
Citrix	UDP	1604
CUSeeMe	TCP	7648, 7649
CUSeeMe	UDP	7648, 7649, 24032
DHCP	UDP	67, 68
DNS	TCP/UDP	53
eDonkey	TCP	4662
Exchange	TCP	135
Fasttrack	TCP	1214
Finger	TCP	79
FTP	TCP	21
Gnutella	TCP	6346, 6347, 6348, 6349, 6355, 5634
Gopher	TCP/UDP	70
H323	TCP	1300, 1718, 1719, 1720, 11000-1999
H323	UDP	1300, 1718, 1719, 1720, 11720
HTTP	TCP	80
IMAP	TCP/UDP	143, 220
IRC	TCP/UDP	194
Kerberos	TCP/UDP	88, 749
L2TP	UDP	1701
LDAP	TCP/UDP	389
Mgcp	TCP	2427, 2428, 2727
Mgcp	UDP	2427, 2727
Napster	TCP	6699, 8875, 8888, 7777, 6700, 6666, 6677, 6688, 4444, 5555

Table 493 Protocols of pre-defined ports

Protocol name	Protocol type	Pre-defined port number
NetBIOS	TCP	137, 138, 139
NetBIOS	UDP	137, 138, 139
Netshow	TCP	1755
NFS	TCP/UDP	2049
NNTP	TCP/UDP	119
Notes	TCP/UDP	1352
Novadign	TCP/UDP	3460, 3461, 3462, 3463, 3464, 3465
NTP	TCP/UDP	123
PCAnywhere	TCP	5631, 65301
PCAnywhere	UDP	22, 5632
POP3	TCP/UDP	110
PPTP	TCP	1723
Printer	TCP/UDP	515
RCMD	TCP	512, 513, 514
RIP	UDP	520
RSVP	UDP	1698, 1699
RTSP	TCP	554
Secure-FTP	TCP	990
Secure-HTTP	TCP	443
Secure-IMAP	TCP/UDP	585, 993
Secure-IRC	TCP/UDP	994
Secure-LDAP	TCP/UDP	636
Secure-NNTP	TCP/UDP	563
Secure-POP3	TCP/UDP	995
Secure-TELNET	TCP	992
SIP	TCP/UDP	5060
Skinny	TCP	2000, 2001, 2002
SMTP	TCP	25
SNMP	TCP/UDP	161, 162
SOCKS	TCP	1080
Sqlnet	TCP	1521
Sqlserver	TCP	1433
SSH	TCP	22
Streamwork	UDP	1558
Sunrpc	TCP/UDP	111
Syslog	UDP	514
Telnet	TCP	23
Tftp	UDP	69
Vdolive	TCP	7000
Winmx	TCP	6699
X Windows	TCP	6000, 6001, 6002, 6003

Description Use the **dar protocol** command to configure the port number of DAR application protocol.

Use the **undo dar protocol** command to restore the port number to default value.

By default, port number is specified for the protocols except for the ten user-defined protocols, RTP and RTCP.

Examples # Set the port number of RTP protocol to 36000, 36001, or 40000 to 40999.

```
<Sysname> system-view
[Sysname] dar protocol rtp udp port 36000 36001 range 40000 40999
```

dar protocol-rename

Syntax **dar protocol-rename** *old-name user-defined-name*

undo dar protocol-rename *user-defined-name*

View System view

Parameters *old-name*: Initial name of the user-defined protocol, which are **user-defined01**, **user-defined02**, ..., **user-defined10.**

user-defined-name: New name of the user-defined protocol, in the length of 1 to 14 characters. The new name cannot be the same with any existing name, and cannot be all, total, tcp, udp, ip or user-defined01, user-defined02, ..., user-defined10.

Description Use the **dar protocol-rename** command to rename the user-defined protocol.

Use the **undo dar protocol-rename** command to restore the default name.

By default, the names of the user-defined protocols are **user-defined01**, **user-defined02**, ..., **user-defined10**.

Examples # Rename the user-defined01 protocol to hello.

```
<Sysname> system-view
[Sysname] dar protocol-rename user-defined01 hello
```

Restore the default name of the user-defined01 protocol.

```
<Sysname> system-view
[Sysname] undo dar protocol-rename hello
```

dar protocol-statistic

Syntax **dar protocol-statistic** [**flow-interval** *time*]

undo dar protocol-statistic

View Interface view

Parameters *time*: Time interval between statistics actions , in minute, in the range 1 to 30. By default, it is 5 minutes.

Description Use the **dar protocol-statistic** command to enable DAR packet statistics function.

Use the **undo dar protocol-statistic** command to disable the function.

With DAR packet statistics function, users can timely monitor the packet number, data stream volume, historical mean rate and historical maximum rate of application protocol on each interface, thus to facilitate implementing corresponding policies for the data streams.

By default, the function is disabled.

Examples # Enable DAR packet statistics function on the interface Ethernet1/0, and set the interval to 7 minutes.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/0
[Sysname-Ethernet1/0] dar protocol-statistic flow-interval 7
```

display dar information

Syntax **display dar information**

View Any view

Parameters None

Description Use the **display dar information** command to display information about the DAR module.

Examples # Display information about the DAR module.

```
<Sysname> display dar information
Max session count       : 65536
Watched session count   : 1000
```

Table 494 Description on the fields of the display dar information command

Field	Description
Max session count	The number of maximum sessions
Watched session count	The number of watched sessions

display dar protocol

Syntax **display dar protocol** { **all** | *protocol-name* }

View Any view

Parameters **all**: Displays information about all protocols.

protocol-name: Displays information about specified protocols, in the same range with the *protocol-name* defined in the **dar protocol** command.

Description Use the **display dar protocol** command to display configuration information about the DAR protocol.

The TCP/UDP port numbers are displayed for the static port protocols and general application layer protocols.

Examples # Display information about all protocols.

```
<Sysname> display dar protocol all
Protocol         TCP/UDP  Port
---------------- -------- -----------
bgp              tcp      179
                 udp      179
bittorrent       tcp      range 6881 6889
citrix           tcp      1494
                 udp      1604
cuseeme          tcp      7648 7649
                 udp      7648 7649 24032
dhcp             udp      67 68
dns              tcp      53
                 udp      53
exchange         tcp      135
fasttrack        tcp      1214
finger           tcp      79
ftp              tcp      21
gnutella         tcp      5634 6355 range 6346 6349
gopher           tcp      70
                 udp      70
h323             tcp      1300 1718 1719 1720 range 11000 11999
                 udp      1300 1718 1719 1720 11720
http             tcp      80
imap             tcp      143 220
                 udp      143 220
irc              tcp      194
                 udp      194
kerberos         tcp      88 749
                 udp      88 749
l2tp             udp      1701
ldap             tcp      389
                 udp      389
mgcp             tcp      2427 2428 2727
                 udp      2427 2727
napster          tcp      6699 8875 8888 7777 6700 6666 6677 6688 4444
```

```
 5555
netbios         tcp      137 138 139
                udp      137 138 139
netshow         tcp      1755
nfs             tcp      2049
                udp      2049
nntp            tcp      119
                udp      119
notes           tcp      1352
                udp      1352
novadign        tcp      3460 3461 3462 3463 3464 3465
                udp      3460 3461 3462 3463 3464 3465
ntp             tcp      123
                udp      123
pcanywhere      tcp      5631 65301
                udp      22 5632
pop3            tcp      110
                udp      110
pptp            tcp      1723
printer         tcp      515
                udp      515
rcmd            tcp      512 513 514
rip             udp      520
rsvp            udp      1698 1699
rtcp
rtp
rtsp            tcp      554
secure-ftp      tcp      990
secure-http     tcp      443
secure-imap     tcp      585 993
                udp      585 993
secure-irc      tcp      994
                udp      994
secure-ldap     tcp      636
                udp      636
secure-nntp     tcp      563
                udp      563
secure-pop3     tcp      995
                udp      995
secure-telnet   tcp      992
sip             tcp      5060
                udp      5060
skinny          tcp      2000 2001 2002
smtp            tcp      25
snmp            tcp      161 162
                udp      161 162
socks           tcp      1080
sqlnet          tcp      1521
sqlserver       tcp      1433
ssh             tcp      22
streamwork      udp      1558
sunrpc          tcp      111
                udp      111
syslog          udp      514
telnet          tcp      23
tftp            udp      69
user-defined01
user-defined02
```

```
user-defined03
user-defined04
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
vdolive         tcp      7000
winmx           tcp      6699
xwindows        tcp      range 6000 6003
```

Table 495 Description on the fields of the display dar protocol command

Field	Description
Protocol	Protocol name
TCP/UDP	Based on TCP/UDP
Port	Port number

display dar protocol-rename

Syntax **display dar protocol-rename**

View Any view

Parameters None

Description Use the **display dar protocol-rename** command to display the rename information of user-defined protocols.

Examples # Display the rename information of user-defined protocols.

```
<Sysname> display dar protocol-rename
Default Name     User Defined Name
---------------- --------------------
user-defined01   merry
user-defined02
user-defined03
user-defined04
user-defined05
user-defined06
user-defined07
user-defined08
user-defined09
user-defined10
```

Table 496 Description on the fields of the display dar protocol-rename command

Field	Description
Default Name	Name of default protocol
User Defined Name	Name of user-defined protocol

display dar protocol-statistic

Syntax **display dar protocol-statistic** [**protocol** *protocol-name* | **top** *top-number* | **all**] [**interface** *interface-type interface-number*] [**direction** { **in** | **out** }]

View Any view

Parameters **protocol** *protocol-name*: Displays specified protocol, in the same range with the *protocol-name* defined in the **if-match protocol** command.

top *top-number*: Displays the newest protocols of the traffic in *top-number*, in the range 1 to 16.

all: Displays all protocol packets; it defaults not to display the statistics packets and the protocol packets in 0 byte.

interface-type interface-number: Specifies an interface by its type and number.

direction: Specifies the direction to display traffic. By default, it is bi-directional.

in: Displays the traffic on the inbound direction.

out: Displays the traffic on the outbound direction.

Description Use the **display dar protocol-statistic** command to display DAR packet statistics information.

Examples # Display statistics information about all protocol packets.

```
<Sysname> display dar protocol-statistic
Interface: Ethernet0/0
Port     In/Out  Packet Count  Byte Count      Bit Rate    Max Bit Rate
                                                in 5 min     in 5 min
                                                (bps)       (bps)
-------- ------ ------------- --------------- ------------ -----------
ftp       IN    33            1034            23           44
          OUT   10            650             0            0
http      IN    24            948             11           20
bgp       IN    1             72              10           12
Total     IN    58            2054            44           76
          OUT   10            650             0            0

Interface: Ethernet2/0
Port     In/Out  Packet Count  Byte Count      Bit Rate    Max Bit Rate
                                                in 5 min     in 5 min
                                          (bps)       (bps)
-------- ------ ------------- --------------- ------------ -----------
bgp       OUT   23            1480            110          112
Total     OUT   23            1480            110          112
```

Table 497 Description on the fields of the display dar protocol-statistic command

Field	Description
Port	Protocol name
In/Out	Direction in which the packet is transmitted (inbound/outbound)

Table 497 Description on the fields of the display dar protocol-statistic command

Field	Description
Packet Count	Packet number
Byte Count	Byte number
Bit Rate in 5 min(bps)	Bit rate within 5 minutes, in bps
Max Bit Rate in 5 min(bps)	Maximum bit rate within 5 minutes, in bps

if-match protocol

Syntax **if-match** [**not**] **protocol** *protocol-name*

undo if-match [**not**] **protocol** *protocol-name*

View Class view

Parameters **not:** Specifies the current rule to not to match the specified matching rule.

protocol-name: Name of matching protocols, in the range **bgp**, **bittorrent**, **citrix**, **cuseeme**, **dhcp**, **dns**, **edonkey**, **egp, eigrp, exchange**, **fasttrack**, **finger**, **ftp**, **gnutella**, **gopher**, **gre, h323**, **icmp**, **igmp**, **imap**, **ip, ipinip**, **ipsec**, **ipv6, irc**, **kerberos**, **l2tp**, **ldap**, **mgcp**, **napster**, **netbios**, **netshow**, **nfs**, **nntp**, **notes**, **novadign**, **ntp**, **pcanywhere**, **pop3**, **pptp**, **printer**, **rcmd**, **rip**, **rsvp**, **rtcp**, **rtsp**, **secure-ftp**, **secure-http**, **secure-imap**, **secure-irc**, **secure-ldap**, **secure-nntp**, **secure-pop3**, **secure-telnet**, **sip**, **skinny**, **smtp**, **snmp**, **socks**, **sqlnet**, **sqlserver**, **ssh**, **streamwork**, **sunrpc** , **syslog**, **telnet**, **tftp**, **vdolive**, **winmx**, **xwindows**, **unknown-tcp**, **unknown-udp**, **unknown-others**, **user-defined01**, **user-defined02**, ..., **user-defined10** (the new names will apply if the protocols **user-defined01** to **user-defined10** are renamed), in which **unknown-tcp** indicates the irrecognizable TCP packet, **unknown-udp** indicates the irrecognizable UDP packet, and **unknown-others** indicates other irrecognizable IP packets. The **user-defined01**, **user-defined02**, ..., **user-defined10** are user-defined protocol packets, whose port numbers are invalid before the **dar protocol** command is executed.

Description Use the **if-match protocol** command to define protocol matching rules.

Use the **undo if-match protocol** command to delete the rules.

By default, no matching rule is configured.

Examples # Define smtp-class and configure the matching rule to match the SMTP protocol.

```
<Sysname> system-view
[Sysname] traffic classifier smtp-class
[Sysname-classifier-smtp-class] if-match protocol smtp
```

if-match protocol http

Syntax **if-match** [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

undo if-match [**not**] **protocol http** [**url** *url-string* | **host** *hostname-string* | **mime** *mime-type*]

View Class view

Parameters **not**: Specifies the current rule to not to match the specified matching rule.

url: Matches according to the URL in the HTTP packet.

url-string: URL for matching in the HTTP packet, which supports simple wildcard character matching, a string of 1 to 32 characters.

host: Matches according to the host name in the HTTP packet.

hostname-string: The host name for matching in the HTTP packet, which supports simple wildcard matching, a string of 1 to 32 characters.

mime: Matches according to the MIME type in the HTTP packet.

mime-type: The MIME type for matching in the HTTP packet, which supports simple wildcard character matching, a string of 1 to 32 characters.

See Table 498 for the matching rules of simple wildcard characters.

Table 498 The matching rules of simple wildcard characters

Character	Description
*	Matching zero character or random several characters, including digit, capital/small letter, hyphen, or underline
#	Matching a character, including digit, capital/small letter, hyphen, or underline.
|	Matching either of the two character strings on the left and right sides
(|)	Matching either of the two character strings on the left and right sides within a certain range. For example, index.(htm|jsp) matches both index.htm and index.jsp
[ ]	Matching any one character specified in the square brackets, or a special character, including *, #, [, (, |, or). For example, [0-9] indicates all digits, [*] indicates *, and [[] indicates [

Description Use the **if-match protocol http** command to configure HTTP matching rules.

Use the **undo if-match protocol http** command to delete the rules.

By default, no matching rule is configured.

Examples # Define the class http-class, and configure the matching rule to be the HTTP packet with the host name *.abc.com.

```
<Sysname> system-view
[Sysname] traffic classifier http-class
[Sysname-classifier-http-class] if-match protocol http host *.abc.com
```

if-match protocol rtp

Syntax **if-match** [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string* } *]

undo if-match [**not**] **protocol rtp** [**payload-type** { **audio** | **video** | *payload-string* }*]

View Class view

Parameters **not**: Specifies the current rule to not to match the specified matching rule.

payload-type: Matches payload type.

audio: Matches the audio RTP payload type.

video: Matches the video RTP payload type.

payload-string: The payload type matched in the RTP packet, in the range 0 to 127. Up to 16 port numbers can be set for each protocol, which are separated with spaces.

Description Use the **if-match protocol rtp** command to configure RTP matching rules.

Use the **undo if-match protocol rtp** command to delete the rules.

If no payload type is specified, it matches all RTP packets.

By default, no RTP matching rule is configured.

Examples # Define the class rtp-class1, and configure the matching rule to be the RTP packet in the audio payload type.

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class1
[Sysname-classifier-rtp-class1] if-match protocol rtp payload-type video
```

Define the class rtp-class2, and configure the matching rule to be the RTP packet in the 0, 1, 4, 5, 6, 10, or 64 payload type.

```
<Sysname> system-view
[Sysname] traffic classifier rtp-class2
[Sysname-classifier-rtp-class2] if-match protocol rtp payload-type 0
 1 4 5 6 10 64
```

reset dar protocol-statistic

Syntax **reset dar protocol-statistic** { { **protocol** *protocol-name* | **interface** *interface-type interface-number* } * | **all** }

View User view

Parameters **protocol** *protocol-name*: Deletes statistics information about specified protocol, in the same range with *protocol-name* in the **if-match protocol** command.

interface-type interface-number: Specifies an interface by its type and number.

all: Deletes all statistics information.

Description Use the **reset dar protocol-statistic** command to delete DAR protocol statistics information, i.e. to restore the statistics to 0.

Examples # Delete FTP protocol statistics information of the interface Ethernet 1/0.

```
<Sysname> reset dar protocol-statistic protocol ftp interface Ethernet 1/0
```

Deletes all statistics information.

```
<Sysname> reset dar protocol-statistic all
```

reset dar session

Syntax **reset dar session**

View User view

Parameters None

Description Use the **reset dar session** command to clear all session connection cache information.

Examples # Delete all session connection cache information.

```
<Sysname> reset dar session
```

125
FR QoS Configuration Commands

apply policy outbound

Syntax **apply policy** *policy-name* **outbound**

undo apply policy outbound

View Frame relay class view

Parameters *policy-name*: Name of the applied policy. It is a string with 1 to 31 characters.

Description Use the **apply policy outbound** command to set the FR virtual circuit queuing to Class-Based Queuing (CBQ).

Use the **undo apply policy outbound** command to restore the FR virtual circuit queuing to FIFO.

By default, FIFO queuing is adopted.

Examples # Define a classifier named class 1.

```
<Sysname> system-view
[Sysname] traffic classifier class1
[Sysname-classifier-class1] quit
```

Define a traffic behavior named behavior 1.

```
[Sysname] traffic behavior behavior1
[Sysname-behavior-behavior1] queue af bandwidth 56
[Sysname-behavior-behavior1] quit
```

Define a policy named policy 1 and associate class 1 with behavior.

```
[Sysname] qos policy policy1
[Sysname-qospolicy-policy1] classifier class1 behavior behavior1
[Sysname-qospolicy-policy1] quit
```

Apply a defined policy to the FR class named test 1 and set the queuing of test 1 to CBQ.

```
[Sysname] fr class test1
[Sysname-fr-class-test1] apply policy policy1 outbound
```

cbs

Syntax **cbs** [**inbound** | **outbound**] *committed-burst-size*

undo cbs [**inbound** | **outbound**]

View Frame relay class view

Parameters **inbound**: Sets the committed burst size of the inbound packet, valid only when Frame Relay Traffic Policing (FRTP) is enabled on the interface.

outbound: Sets the committed burst size of the outbound packet, valid only when Frame Relay Traffic Shaping (FRTS) is enabled on the interface.

committed-burst-size: Committed burst size, in bits, ranging from 300 to 16000000. It defaults to 56000 bits.

Description Use the **cbs** command to set the committed burst size of FR virtual circuit.

Use the **undo cbs** command to restore the default value.

If the packet direction is not specified in configuration, the parameter will be set in both inbound and outbound directions.

The committed burst size is the packet traffic that is committed to send on a FR network within an interval of Tc. When there is no congestion on the network, the FR network ensures this part of traffic could be sent successfully.

Related commands: **ebs**, **cir allow**, **cir**.

Examples # Set the committed burst size of the FR class named test1 as 64000 bits.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cbs 64000
```

cir

Syntax **cir** *committed-information-rate*

undo cir

View Frame relay class view

Parameters *committed-information-rate*: The minimum committed information rate (CIR), in bps, ranging from 1000 to 45000000. It defaults to 56000 bps.

Description Use the **cir** command to set the CIR of FR virtual circuit.

Use the **undo cir** command to restore the default value.

The CIR is the minimum sending rate that can be provided by virtual circuit. It ensures the user could still send data at this rate upon network congestion.

Upon network congestion, DCE will send a packet with a BECN flag bit of 1 to DTE. After DTE receives this packet, it gradually reduces the sending rate of virtual circuit from the allowed CIR (CIR ALLOW) to CIR. If DTE does not receive the packet with the BECN flag bit of 1 any more within a certain period of time, it will restore the sending rate of virtual circuit as CIR ALLOW.

The CIR must not exceed the CIR ALLOW.

Related commands: **cbs**, **ebs**, **cir allow**.

Examples # Set the CIR of the FR class named test1 as 32000 bps.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir 32000
```

cir allow

Syntax **cir allow** [**inbound** | **outbound**] *committed-information-rate*

undo cir allow [**inbound** | **outbound**]

View Frame relay class view

Parameters **inbound**: Sets the CIR ALLOW of an inbound packet, valid only when FRTP is enabled on the interface.

outbound: Sets the CIR ALLOW of an outbound packet, valid only when FRTS is enabled on the interface.

committed-information-rate: CIR ALLOW, in bps, ranging from 1000 to 45000000. It defaults to 56000 bps.

Description Use the **cir allow** command to set the CIR ALLOW of FR virtual circuit.

Use the **undo cir allow** command to restore the default value.

CIR ALLOW is the sending rate that can be normally provided by a FR network. When there is no congestion on the network, it ensures the user could send data at this rate.

If packet direction is not specified upon configuration, the parameter will be set in both inbound and outbound directions.

The CIR must not exceed the CIR ALLOW.

Related commands: **cbs**, **ebs**, **cir**.

Examples # Set the CIR ALLOW of the FR class that is named test1 as 64000 bps.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cir allow 64000
```

congestion-threshold

Syntax **congestion-threshold** { **de** | **ecn** } *queue-percentage*

undo congestion-threshold { **de** | **ecn** }

View Frame relay class view

Parameters **de**: Discards the FR packet whose DE flag bit is 1 upon congestion.

ecn: Processes the flag bits, BECN and FECN, of FR packet upon congestion.

queue-percentage: Network congestion threshold, the utility ratio of virtual circuit queue, namely the percentage of the current queue length of virtual circuit to the total queue length, ranging from 1 to 100. By default, it is 100.

Description Use the **congestion-threshold** command to enable congestion management function of FR virtual circuit.

Use the **undo congestion-threshold** command to disable this function.

When the percentage of current queue length to the total queue length of virtual circuit exceeds the set congestion threshold, it will be regarded that congestion occurs on the virtual circuit and congestion management will be performed on packets on virtual circuit.

Related commands: **fr congestion-threshold**.

Examples # Set to discard the FR packet whose DE flag bit is 1 concerning the FR class named test1, when the current queue length of virtual circuit exceeds 80% of the total length.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] congestion-threshold de 80
```

cq

Syntax **cq cql** *cql-index*

undo cq

View Frame relay class view

Parameters **cql** *cql-index*: Group number of Custom Queuing, ranging from 1 to 16.

Description Use the **cq** command to set the FR virtual circuit queuing to Custom Queuing (CQ).

Use the **undo cq** command to restore the FR virtual circuit queuing to FIFO.

By default, the virtual circuit queuing type is FIFO.

If you use this command repeatedly on the same FR, the new configuration will overwrite the old one.

Related commands: **wfq**, **pq**, **fr pvc-pq**.

Examples # Apply the group10 of Custom Queuing to the FR class named test1.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] cq cql 10
```

display fr class-map

Syntax **display fr class-map** { **fr-class** *class-name* | **interface** *interface-type interface-number* }

View Any view

Parameters *class-name*: FR class name, a string of 1 to 30 characters.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **display fr class-map** command to view information on FR class to interface map, including DLCIs of interfaces, subinterfaces on the interfaces and their DLCIs.

When configuring the command, you can specify a FR class name or main interface, but not a subinterface.

Examples # Display information on the map of FR class to the interface Serial1/0.

```
<Sysname> display fr class-map interface Serial 1/0
Serial1/0
  fr-class ts
  Serial1/0.1
    fr-class ts
    fr dlci  100    Serial1/0
    fr-class ts
    fr dlci 200    Serial1/0.1
      fr-class ts
```

Table 499 Description on the fields of the display fr class-map command

Field	Description
Serial1/0	FR interface
The first fr-class	FR class on FR interface
Serial1/0.1	Subinterface on the FR interface
The second fr-class	FR class on FR subinterface
fr dlci 100 Serial1/0	Virtual circuit on FR interface, specifying the virtual circuit belongs to the main interface or the subinterface.
The third fr-class	FR class associated with virtual circuit on the FR interface

Display information on the map of FR class ts to interfaces.

```
<Sysname> display fr class-map fr-class ts
Serial1/0
  fr-class ts
  Serial1/0.1
    fr-class ts
    fr dlci 100    Serial1/0
    fr-class ts
    fr dlci 200    Serial1/0.1
      fr-class ts
```

Table 500 Description on the fields of the display fr class-map command

Field	Description
Serial1/0	FR interface
The first fr-class ts	FR class configured on the FR interface
Serial1/0.1	Subinterface on the FR interface
The second fr-class	FR class on FR subinterface
fr dlci 100 Serial1/0	Virtual circuit on FR interface, specifying the virtual circuit belongs to the main interface or the subinterface.
The third fr-class ts	FR class associated with virtual circuit on the FR interface

display fr fragment-info

Syntax **display fr fragment-info** [**interface** *interface-type interface-number*] [*dlci-number*]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

dlci-number: DLCI number, ranging from 16 to 1007. The detailed information will be displayed when specifying the parameter.

Description Use the **display fr fragment-info** command to view the FR fragment information.

Related commands: **fragment**.

Examples # Display FR fragment information of all the interfaces.

```
<Sysname> display fr fragment-info
interface Serial1/0:1:
dlci     type                 size         in/out/drop
200      FRF12(End to End)    80            0/0/0
```

Table 501 Description on the fields of the display fr fragment-info command

Field	Description
interface	Interface
dlci	DLCI number
type	Fragment type. Three options are available: FRF.12, FRF.11 Annex C and Motorola fragment.
size	Fragment size
in/out/drop	Number of received fragment packets/number of sent fragment packets/number of discarded fragment packets

Display FR fragment information of a certain interfaces.

```
<Sysname> display fr fragment-info interface Serial 1/0:1 200
Type : FRF12(End to End)
 Size : 80
Data-level: 200    Voice-level: 0
 Pre-fragment:
    out pkts : 0             out bytes :0
 Fragmented:
    in pkts : 0            out pkts : 0
    in bytes: 0            out bytes: 0
 Assembled:
    in pkts : 0            in bytes :0
 Dropped   :
    in pkts : 0            out pkts :0
    in bytes: 0            out bytes: 0
 Out-of-sequence pkts: 0
```

Table 502 Description on the fields of the display fr fragment-info interface

Field	Description
Type	Fragment type. Three options are available: FRF.12, FRF.11 Annex C and Motorola fragment.
Size	Fragment size
Data-level	Fragment size before voice is enabled
Voice-level	Fragment size when voice is enabled
Pre-fragment	Number of packets and bytes to send before fragmented
Fragmented	Number of fragments received and sent counted in packet and byte.
Assembled	Number of assembled fragments
Dropped	Number of dropped fragments
Out-of-sequence pkts	Number of out-of-order fragments
out pkts / out bytes	Number of outgoing packets/bytes
in pkts / in bytes	Number of incoming packets/bytes

display fr switch-table

Syntax **display fr switch-table** { **all** | **name** *switch-name* | **interface** *interface-type interface-number* }

View Any view

Parameters **all**: All the PVC information

name: PVC information of a specified name.

switch-name: PVC name, in the range 1 to 256 characters.

interface: PVC information of a specified interface.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **display fr switch-table** command to view configuration and status information of the FR route to confirm the correctness of the configuration.

Related commands: **fr switch**.

Examples # Display all FR PVC information.

```
<Sysname> display fr switch-table all
Switch-Name     Interface      DLCI  Interface          DLCI  State
  test           MFR1/0        100    MFR1/1            101   UP
```

Table 503 Description on the fields of the display fr switch-table command

Field	Description
Switch-Name	Name of PVC used for switching
Interface	The first denotes local interface and the second denotes remote interface
DLCI	local and remote VC identifier
State	Linkage status

display qos policy interface

Syntax **display qos policy interface** [*interface-type interface-number* [**dlci** *dlci-number* [**user-defined**] | **inbound** | **outbound**]]

View Any view

Parameters *interface-type interface-number*: Specifies an interface by its type and number.

dlci: Information about the specified DLCI applying CBQ.

dlci-number: DLCI number, in the range 16 to 1007.

user-defined: User-defined DLCI.

inbound: Information about inbound interface applying CBQ.

outbound: Information about outbound interface applying CBQ.

Description Use the **display qos policy interface** command to view information about CBQ application on the interface.

Examples # Display the information about CBQ application of the virtual circuit with DLCI of 25 on interface MFR1/0.

```
<Sysname> display qos policy interface mfr1/0
MFR1/0, DLCI 25
  Direction: Outbound

  Policy: xujin

   Classifier: default-class
    Matched : 1/133 (Packets/Bytes)
    Rule(s) : if-match any
    Behavior:
    Default Queue:
      Flow Based Weighted Fair Queueing
        Max number of hashed queues: 256
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes)
        Discard Method: Tail

   Classifier: xujin
    Matched : 0/0 (Packets/Bytes)
    Operator: Logic AND
    Rule(s):  if-match acl 2001
    Behavior:
      Assured Forwarding:
        Bandwidth 10 (Kbps)
        Matched  : 0/0 (Packets/Bytes)
        Enqueued : 0/0 (Packets/Bytes)
        Discarded: 0/0 (Packets/Bytes
```

Table 504 Description on the fields of the display qos policy interface command

Field	Description
MFR1/0, DLCI 25	FR interface and virtual circuit with CBQ applied
Direction	Direction of the interface to which a policy is applied
Policy	Name of the policy applied on an interface
Classifier	Classification rule and the corresponding configuration information for a policy
Matched	Number of packets matching a classification rule
Operator	Logic relationship among multiple classification rules in a class
Rule(s)	Matching rule of a class
Behavior	Behavior name and the corresponding configuration information in a policy
Default Queue	Default queue
Flow Based Weighted Fair Queueing	Flow based weighted fair queueing

Table 504 Description on the fields of the display qos policy interface command

Field	Description
Max number of hashed queues	Max number of hashed queues
Matched	Number of matched packets or bytes for a queue
Enqueued	Number of enqueued packets or bytes
Discarded	Number of discarded packets or bytes
Discard Method	Discard method
Assured Forwarding	Information of assured forwarding queue
Bandwidth	The minimum bandwidth of an AF queue

display qos pvc-pq interface

Syntax **display qos pvc-pq interface** [*interface-type interface-number*]

View Any view

Parameters *interface-type interface-number:* Specifies an interface by its type and number.

Description Use the **display qos pvc-pq interface** command to view the information about the PVC PQ on FR interface.

Examples # Display PVC PQ information on FR interface Serial2/0.

```
<Sysname> display qos pvc-pq interface serial 2/0
Interface: Serial2/0
Output queue : (Protocol queuing : Size/Length/Discards)  0/500/0
Output queue : (PVC-PQ queue : Size/Length/Discards)
Top:  0/20/0    Middle:  0/40/0    Normal:  0/60/0    Bottom:  0/80/0
```

Table 505 Description on the fields of the display qos pvc-pq interface command

Item	Description
Interface	FR interface
Output queue : (Protocol queuing : Size/Length/Discards)	Output queue information for protocol queuing: Packet size/queue length/number of discarded packets
Output queue : (PVC-PQ queue : Size/Length/Discards)	Output queue information for PVC-PQ queuing: Packet size/queue length/number of discarded packets
Top	Output queue information for high priority queuing
Middle	Output queue information for middle priority queuing
Normal	Output queue information for normal priority queuing
Bottom	Output queue information for low priority queuing

ebs

Syntax **ebs** [**inbound** | **outbound**] *excess-burst-size*

undo ebs [**inbound** | **outbound**]

View Frame relay class view

Parameters **inbound**: Sets the EBS in inbound direction, valid only when FRTP is enabled on the interface.

outbound: Sets EBS in outbound direction, valid only when FRTS is enabled on the interface.

excess-burst-size: EBS in bit, ranging from 0 to 16000000. It defaults to 0 bit.

Description Use the **ebs** command to set EBS of FR virtual circuit.

Use the **undo ebs** command to restore the default value.

EBS is the maximum of the part that packet traffic exceeds the committed burst size (CBS) within an interval of Tc. When congestion occurs on the network, this part of excess traffic will be first discarded.

When this command is used, the set EBS value will be valid in both inbound and outbound directions if the parameters **inbound** and **outbound** are not specified.

Related commands: **cbs**, **cir allow**, **cir**.

Examples # Set the EBS of the FR class named test1 to 32000 bits.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] ebs 32000
```

fifo queue-length

Syntax **fifo queue-length** *queue-length*

undo fifo queue-length

View Frame relay class view

Parameters *queue-length*: FIFO queue length, namely, the maximum number of packets that can be held by the queue, ranging from 1 to 1024. By default, it is 40.

Description Use the **fifo queue-length** command to set the FIFO queue length of FR virtual circuit.

Use the **undo fifo queue-length** command to restore the default value.

When the router serves as DCE for switching, the FIFO queue length of DLCI can be set if FRTS has been applied to DLCI.

Related commands: **fr class**.

Examples # Set the FIFO queue of the FR class named test1 to hold 80 packets at most.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fifo queue-length 80
```

fr class

Syntax **fr class** *class-name*

undo fr class *class-name*

View System view

Parameters *class-name*: FR class name, a string of 1 to 30 characters.

Description Use the **fr class** command to create a FR class and enter FR class view.

Use the **undo fr class** command to delete a specified FR class.

By default, no FR class is created.

Only after associating a FR class with an interface or virtual circuit and enabling the FR QoS function on the corresponding interface, can the set FR class parameter take effect.

When a FR class is deleted, the association between all interfaces or DLCIs and the FR class will be released.

Related commands: **fr-class**.

Examples # Create a FR class named test1.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1]
```

fr congestion-threshold

Syntax **fr congestion-threshold** { **de** | **ecn** } *queue-percentage*

undo fr congestion-threshold { **de** | **ecn** }

View Frame relay interface view, MFR interface view

Parameters **de**: Discards the FR packet whose DE flag bit is 1 when congestion occurs.

ecn: Processes the BECN and FECN flag bits of FR packets when congestion occurs.

queue-percentage: Network congestion threshold, the occupation ratio of the interface queue, equal to the percentage of current queue length to the total queue length of the interface, ranging from 1 to 100. By default, it is 100.

Description Use the **fr congestion-threshold** command to enable congestion management function of a FR interface.

Use the **undo fr congestion-threshold** command to disable this function.

By default, the congestion management function of a FR interface is disabled.

This command is similar to the **congestion-threshold** command. The difference is that this command is applied to FR interfaces, while the **congestion-threshold** command is applied to FR virtual circuit.

The command can only be used for FR DCE interfaces or NNI interfaces.

Related commands: **congestion-threshold**.

Examples # Set to process the flag bit of a FR packet when the interface queue length exceeds 80% of the total length.

```
<Sysname> system-view
[Sysname]interface Serial 1/0
[Sysname-Serial1/0] fr congestion-threshold de 80
```

fr de del

Syntax **fr de del** *list-number* **dlci** *dlci-number*

undo fr de del *list-number* **dlci** *dlci-number*

View Frame relay interface (main interface or subinterface) view, MFR interface view

Parameters *list-number*: DE rule list number, ranging from 1 to 10.

dlci-number: Frame relay virtual circuit number, ranging from 16 to 1007.

Description Use the **fr de del** command to apply a DE rule list to the specified FR virtual circuit.

Use the **undo fr de del** command to delete a DE rule list from virtual circuit.

By default, no DE rule list is applied to FR virtual circuit.

In the view of a FR main interface (or subinterface), this command can only apply a DE rule list to the FR VCs on the main interface or (or subinterface).

After a DE rule list is applied to FR virtual circuit, those packets that match the rule list will have their DE flag set to 1.

Related commands: **fr del inbound-interface**, **fr del protocol**.

Examples # In the view of interface Serial 1/0, apply DE rule list 3 to DLCI 100 on the current interface.

```
<Sysname> system-view
[Sysname]interface Serial 1/0
[Sysname-Serial1/0] fr dlci 100
[Sysname-Serial1/0] fr de del 3 dlci 100
```

fr del inbound-interface

Syntax **fr del** *list-number* **inbound-interface** *interface-type interface-number*

undo fr del *list-number* **inbound-interface** *interface-type interface-number*

View System view

Parameters *list-number*: Number of DE rule list, ranging from 1 to 10.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **fr del inbound-interface** command to configure an interface-based DE rule list. For the packet received from the specified interface, if it is forwarded from the router as a FR packet, its DE flag bit is set to 1 before being forwarded.

Use the **undo fr del inbound-interface** command to delete the specified DE rule from a DE rule list.

By default, no DE rule list is created.

New rules can be added to a DE rule list by using this command repeatedly. Up to 100 rules can be configured in a DE rule list. The **undo** form of this command can once delete one DE rule only. To delete a DE rule list, you should first delete all DE rules in it.

Related commands: **fr de del**, **fr del protocol**.

Examples # Add a rule to DE rule list 1. For the packet received from the interface Serial 1/0, if it is needed to be forwarded by encapsulating FR protocol, flag the DE flag bit of the packet as 1 before forwarding.

```
<Sysname> system-view
[Sysname] fr del 1 inbound-interface Serial 1/0
```

fr del protocol

Syntax **fr del** *list-number* **protocol ip** [**acl** *acl-number* | **fragments** | **greater-than** *bytes* | **less-than** *bytes* | **tcp** *ports* | **udp** *ports*]

undo fr del *list-number* **protocol ip** [**fragments** | **acl** *acl-number* | **less-than** *bytes* | **greater-than** *bytes* | **tcp** *ports* | **udp** *ports*]

View System view

Parameters *list-number*: DE rule list number, ranging from 1 to 10.

protocol ip: IP.

fragments: All fragmented IP packets.

acl *acl-number*: IP packets meeting ACL matching requirement. *acl-number* ranges from 2000 to 3999.

less-than *bytes*: IP packets whose length is less than *bytes. bytes* ranges from 0 to 65535.

greater-than *bytes*: IP packets whose length is greater than *bytes*. *bytes* ranges from 0 to 65535.

tcp *ports*: IP packets whose source or destination TCP port number are *ports*, in the range 0 to 65535. The value of ports can be a port name or the related port number. **udp** *ports*: IP packets whose source or destination UDP port number are *ports*, in the range 0 to 65535. The value of ports can be a port name or the related port number. If optional parameters are not used, it represents all IP packets.

Description Use the **fr del protocol ip** command to configure an IP-based DE rule list. The DE flag bit of the FR packet encapsulated with an IP packet matching the specified rule will be flagged as 1.

Use the **undo fr del protocol ip** command to delete the specified DE rule from a DE rule list.

By default, no DE rule list is created.

New rules can be added to a DE rule list by using this command repeatedly. Up to 100 rules can be configured in a DE rule list. The **undo** form of this command can once delete one DE rule only. To delete a DE rule list, you must delete all DE rules in it.

Related commands: **fr de del**, **fr del inbound-interface**.

Examples # Add a rule to DE rule list 1. For all FR packets encapsulated with IP packets, flag their DE flag bits as 1.

```
<Sysname> system-view
[Sysname] fr del 1 protocol ip
```

fr pvc-pq

Syntax **fr pvc-pq** [*top-limit middle-limit normal-limit bottom-limit*]

undo fr pvc-pq

View Frame relay interface view, MFR interface view

Parameters *top-limit*: Length of top priority queue, ranging from 1 to 1024. The value is the number of packets. By default, it is 20.

middle-limit: Length of middle priority queue, ranging from 1 to 1024. The value is the number of packets. By default, it is 40.

normal-limit: Length of normal priority queue, ranging from 1 to 1024. The value is the number of packets. By default, it is 60.

bottom-limit: Length of bottom priority queue, ranging from 1 to 1024. The value is the number of packets. By default, it is 80.

Description Use the **fr pvc-pq** command to set the queue type of a FR interface as PVC PQ (PVC Priority Queuing) and set queue length, i.e. the maximum number of packets that can be held by a queue, for each queue.

Use the **undo fr pvc-pq** command to restore the queue type of the interface into FIFO.

By default, the queuing type of a FR interface is FIFO.

After FRTS is enabled on an interface, the queuing type of the interface can only be FIFO or PVC PQ.

PVC PQ is a new queuing mechanism of FRTS. Similar to PQ, it also has four queue types: top, middle, normal and bottom, in descending order. Configure the queue of PVC PQ that DLCI enters in FR class. When congestion occurs on an interface, different DLCIs enter different PVC PQs. When sending data, according to queue priority, data in higher priority queues will be sent before lower priority queues.

Related commands: **pvc-pq**.

Examples # Set the queuing type of the interface Serial 1/0/ as PVC PQ.

```
<Sysname> system-view
[Sysname] interface Serial 1/0
[Sysname-Serial1/0] fr pvc-pq
```

fr traffic-policing

Syntax **fr traffic-policing**

undo fr traffic-policing

View Frame relay interface view, MFR interface view

Parameters None

Description Use the **fr traffic-policing** command to enable FRTP function.

Use the **undo fr traffic-policing** command to disable FRTP function.

FRTP function is applied to the inbound interface of FR packets on a router. Furthermore, it is only used at the DCE end of a FR network.

When configuring traffic policing for an inbound interface, you must first set the DCE as a FR switching by using the **fr switching** command.

Related commands: **fr class**.

Examples # Enable the traffic policing function on the interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface Serial 1/0
[Sysname-Serial1/0] fr traffic-policing
```

fr traffic-shaping

Syntax **fr traffic-shaping**

undo fr traffic-shaping

View Frame relay interface view, MFR interface view

Parameters None

Description Use the **fr traffic-shaping** command to enable FRTS function.

Use the **undo fr traffic-shaping** command to disable FRTS function.

By default, FRTS function is disabled.

The FRTS function is applied to the outbound interface of a router, generally used at the DTE end of a FR network.

Related commands: **fr class**, **fr-class**, **fr dlci**.

Examples # Enable FRTS on the serial interface Serial 1/0.

```
<Sysname> system-view
[Sysname] interface Serial1/0
[Sysname-Serial1/0] fr traffic-shaping
```

fragment

Syntax **fragment** [*fragment-size*]

undo fragment [*fragment-size*]

View Frame relay class view

Parameters *fragment-size*: Size of a fragment, in byte, ranging from 16 to 1600. By default, the fragment size is of 45 bytes.

Description Use the **fragment** command to enable the FRF.12-compliant fragmentation function on FR virtual circuit.

Use the **undo fragment** command to disable this function.

By default, the fragmentation function on FR virtual circuit is disabled.

Related commands: **fr class**.

Examples # Configure fragment size as 128 in the FR class named test1.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] fragment 128
```

fr-class

Syntax **fr-class** *class-name*

undo fr-class *class-name*

View Frame relay DLCI view/Frame relay interface view

Parameters *class-name*: Name of a FR class, a string of 1 to 30 characters.

Description Use the **fr-class** command to associate a FR class with the current FR virtual circuit or FR interface.

Use the **undo fr-class** command to remove the association between a FR class and the FR virtual circuit or FR interface.

By default, there is no association between a FR class and the FR virtual circuit or FR interface.

If the specified FR class does not exist, the command will first create a FR class before associating the FR class with the current virtual circuit or interface. If the specified FR class does exist, the command will associate the FR class with the current virtual circuit or interface without creating a new FR class.

The **undo** command only removes the association between a specified FR class and a virtual circuit or an interface rather than deletes the real FR class. To delete a FR class, use the **undo fr class** command.

After a FR class is associated with an interface, all virtual circuits on the interface will inherit the FR QoS parameter of this FR class.

Related commands: **fr class**, **fr dlci**.

Examples # Associate the FR class named test1 with the FR virtual circuit whose DLCI is 200.

```
<Sysname> system-view
[Sysname] interface Serial 1/0
[Sysname-Serial1/0] fr dlci 200
[Sysname-fr-dlci-Serial1/0-200] fr-class test1
```

pq

Syntax **pq pql** *pql-index*

undo pq

View Frame relay class view

Parameters *pql-index*: Group number of Priority Queuing, ranging from 1 to 16.

Description Use the **pq** command to set the queue type of FR virtual circuit as Priority Queuing.

Use the **undo pq** command to restore the queue type of virtual circuit to FIFO.

By default, the queuing type of FR virtual circuit is FIFO.

Related commands: **cq**, **wfq**, **fr pvc-pq**.

Examples # Apply the group10 of Priority Queuing to the FR class named test1.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pq pql 10
```

pvc-pq

Syntax **pvc-pq** { **bottom** | **middle** | **normal** | **top** }

undo pvc-pq

View Frame relay class view

Parameters **top**: Sets the top PVC PQ , namely, top priority queue, to accept the packets from the VC.

middle: Sets the middle PVC PQ , namely, middle priority queue, to accept the packets.

normal: Sets the normal PVC PQ , namely, normal priority queue, to accept the packets.

bottom: Sets the bottom PVC PQ , namely, normal priority queue, to accept the packets.

Description Use the **pvc-pq** command to set the type of the PVC PQ that packets sent by FR virtual circuit enter.

Use the **undo pvc-pq** command to restore the default PVC PQ type.

By default, the packets sent by FR virtual circuit enter into the **normal** PVC PQ.

PVC PQ falls into four groups: **top**, **middle**, **normal** and **bottom**. PVC PQ is relative to DLCI. After the queue of an interface is set as PVC PQ, packets on each virtual circuit can enter only one type of PVC PQ.

Related commands: **fr pvc-pq**.

Examples # Set packets sent by virtual circuit which is associated with the FR class named test1 to enter top PVC PQ.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] pvc-pq top
```

rtpq

Syntax **rtpq start-port** *min-dest-port* **end-port** *max-dest-port* **bandwidth** *bandwidth*

undo rtpq

Parameters **start-port** *min-dest-port*: Specifies the lower limit for the destination UDP port number, in the range 2000 to 65535.

end-port *max-dest-port*: Specifies the upper limit for the destination UDP port number, in the range 2000 to 65535.

bandwidth *bandwidth*: Bandwidth of a RTP queue, in kbps, ranging from 8 to 1000000.

View Frame relay class view

Description Use the **rtpq** command to configure to apply Realtime Transport Protocol (RTP) Priority Queuing.

Use the **undo rtpq** command to remove the application.

The application of a FR class configured with RTPQ to a PVC results in the creation of a strict priority queue on the PVC. Packets in the port range specified by RTPQ of the destination UDP port will enter RTPQ. When congestion occurs in the virtual circuit, the packets in the queue will be absolutely sent with preference without exceeding the configured bandwidth. When congestion does not occur in the virtual circuit, the RTP packets in the specified port range can occupy the available bandwidth on the virtual circuit. Generally, the UDP port range used by VoIP can be configured as from 16384 to 32767.

Examples # Configure RTP priority queue on the FR class named test1 with a bandwidth of 20 kbps.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] rtpq start-port 16383 end-port 16384 bandwidth 20
```

traffic-shaping adaptation

Syntax **traffic-shaping adaptation** { **becn** *percentage* | **interface-congestion** *number* }

undo traffic-shaping adaptation { **becn** | **interface-congestion** }

View Frame relay class view

Parameters **becn**: Adjusts the packets with the BECN flag.

percentage: Adjustment percentage, ranging from 1 to 30 percent. The default value is 25 percent.

interface-congestion: Traffic shaping according to the number of the packets in the outbound queue.

number: Number of packets in the queue, ranging from 1 to 40.

Description Use the **traffic-shaping adaptation** command to enable the adaptive traffic shaping function of FR.

Use the **undo traffic-shaping adaptation** command to disable this function.

By default, traffic-shaping adaptation is enabled, and the ratio of each adaptation is set to 25.

Related commands **fr traffic-shaping**, **cir allow**, and **cir**.

Examples # Enable the FR traffic shaping function, by adjusting the packets with the BECN flag 1 and the ratio of each adaptation is set to 20.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] traffic-shaping adaptation becn 20
```

wfq

Syntax **wfq** [*congestive-discard-threshold* [*dynamic-queues*]]

undo wfq

View Frame relay class view

Parameters *congestive-discard-threshold*: The maximum number of packets allowed in the queue. Packets exceeding this limitation will be discarded. The permitted value ranges from 1 to 1024, with a default of 64.

dynamic-queues: Total number of queues, the value can be one of 16, 32, 64, 128, 256, 512, 1024, 2048 and 4096, with the default of 256.

Description Use the **wfq** command to set the queue type of the VC to be WFQ.

Use the **undo wfq** command to restore the queue type to FIFO.

By default, the virtual circuit queuing type is FIFO.

Related commands: **cq**, **pq**, **fr pvc-pq**.

Examples # Apply WFQ to the FR class test1.

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] wfq 128 512
```

126 802.1X CONFIGURATION COMMANDS

display dot1x

Syntax **display dot1x** [**sessions** | **statistics**] [**interface** *interface-list*]

View Any view

Parameter **sessions**: Displays 802.1x session information.

statistics: Displays 802.1x statistics.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **display dot1x** command to display information about 802.1x, including session information, statistics, or configuration.

With both the **sessions** keyword and the **statistics** keyword not provided, this command displays 802.1x configuration information.

Related commands: **reset dot1x statistics**, **dot1x**, **dot1x retry**, **dot1x max-user**, **dot1x port-control**, **dot1x port-method**, **dot1x timer**.

Example # Display 802.1x configuration information.

```
<Sysname> display dot1x
Global Equipment 802.1X protocol is enabled
CHAP authentication is enabled
Proxy trap checker is disabled
Proxy logoff checker is disabled

Configuration: Transmit Period     30 s,  Handshake Period       15 s
               Quiet Period        60 s,  Quiet Period Timer is disabled
               Supp Timeout        30 s,  Server Timeout         100 s
               The maximal retransmitting times          3

Total maximum 802.1x user resource number is 1024 per slot
Total current used 802.1x resource number is 0

Ethernet1/1  is link-up
  802.1X protocol is disabled
```

```
Proxy trap checker is disabled
Proxy logoff checker is disabled
Handshake is disabled
The port is an authenticator
Authenticate Mode is Auto
Port Control Type is Mac-based
Guest VLAN: 0
Max on-line user number is 256
EAPOL Packet: Tx 0, Rx 0
Sent EAP Request/Identity Packets : 0
     EAP Request/Challenge Packets: 0
     EAP Success Packets: 0, Fail Packets: 0
Received EAPOL Start Packets : 0
         EAPOL LogOff Packets: 0
         EAP Response/Identity Packets : 0
         EAP Response/Challenge Packets: 0
         Error Packets: 0

Controlled User(s) amount to 0
```

Table 506 Descriptions on the fields of the display dot1x command

Field	Description
Global Equipment 802.1X protocol is enabled	Indicates whether 802.1x is enabled
CHAP authentication is enabled	Indicates whether CHAP authentication is enabled
Proxy trap checker is disabled	Indicates whether the device is configured to send a trap packet when detecting that a user is trying to login through a proxy
Proxy logoff checker is disabled	Indicates whether the device is configured to get offline any user trying to login through a proxy
Transmit Period	Setting of the username request timeout timer
Handshake Period	Setting of the handshake timer
Quiet Period	Setting of the quiet timer
Quiet Period Timer is disabled	Indicates whether the quiet timer is enabled
Supp Timeout	Setting of the supplicant timeout timer
Server Timeout	Setting of the server timeout timer
The maximal retransmitting times	Maximum number of attempts for the authenticator to send authentication requests to the supplicant
Total maximum 802.1x user resource number per slot	Maximum number of supplicants supported per board
Total current used 802.1x resource number	Total number of online users
Ethernet1/1 is link-up	Status of port Ethernet 1/1
802.1X protocol is disabled	Indicates whether 802.1x is enabled on the port
Proxy trap checker is disabled	Indicates whether the port is configured to send a trap packet when detecting that a user is trying to login through a proxy
Proxy logoff checker is disabled	Indicates whether the port is configured to get offline any user trying to login through a proxy

Table 506 Descriptions on the fields of the display dot1x command

Field	Description
Handshake is disabled	Indicates whether handshake is enabled on the port
The port is an authenticator	Role of the port
Authenticate Mode is Auto	Access control mode for the port
Port Control Type is Mac-based	Access control method for the port
Guest VLAN	Guest VLAN configured for the port. The value of 0 means that no guest VLAN is configured.
Max on-line user number	Maximum number of users supported on the port
EAPOL Packet	Number of EAPOL packets received (Tx) or sent (Rx)
Sent EAP Request/Identity Packets	Number of EAP Request/Identity packets sent
EAP Request/Challenge Packets	Number of EAP Request/Challenge packets sent
EAP Success Packets	Number of EAP Success packets sent
Received EAPOL Start Packets	Number of EAPOL Start packets received
EAPOL LogOff Packets	Number of EAPOL LogOff packets received
EAP Response/Identity Packets	Number of EAP Response/Identity packets received
EAP Response/Challenge Packets	Number of EAP Response/Challenge packets received
Error Packets	Number of erroneous packets received
Controlled User(s) amount	Number of controlled users on the port

dot1x

Syntax In system view:

dot1x [**interface** *interface-list*]

undo dot1x [**interface** *interface-list*]

In Ethernet interface view:

dot1x

undo dot1x

View System view/interface view

Parameter **interface** *interface-list*: Specifies a port list, which can contain multiple ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where

interface-type represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x** command in system view to enable 802.1x globally.

Use the **undo dot1x** command in system view to disable 802.1x globally.

Use the **dot1x interface** *interface-list* command in system view or the **dot1x** command in interface view to enable 802.1x for specified ports.

Use the **undo dot1x interface** *interface-list* command in system view or the **undo dot1x** command in interface view to disable 802.1x for specified ports.

By default, 802.1x is neither enabled globally nor enabled for any port.

Note that:

- 802.1x must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not function.
- You can configure 802.1x parameters either before or after enabling 802.1x.

Related command: **display dot1x**.

Example # Enable 802.1x for ports Ethernet 1/0, and Ethernet 1/5 to Ethernet 1/7.

```
<Sysname> system-view
[Sysname] dot1x interface ethernet 1/0 ethernet 1/5 to ethernet 1/7
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] dot1x
[Sysname-Ethernet1/0] quit
[Sysname] interface ethernet 1/5
[Sysname-Ethernet1/0] dot1x
[Sysname-Ethernet1/0] quit
[Sysname] interface ethernet 1/6
[Sysname-Ethernet1/0] dot1x
[Sysname-Ethernet1/0] quit
[Sysname] interface ethernet 1/7
[Sysname-Ethernet1/0] dot1x
```

Enable 802.1x globally.

```
<Sysname> system-view
[Sysname] dot1x
```

dot1x authentication-method

Syntax **dot1x authentication-method** { **chap** | **eap** | **pap** }

undo dot1x authentication-method

View System view

Parameter **chap**: Authenticates supplicants using CHAP.

eap: Authenticates supplicants using EAP.

pap: Authenticates supplicants using PAP.

Description Use the **dot1x authentication-method** command to set the 802.1x authentication method.

Use the **undo dot1x authentication-method** command to restore the default.

By default, CHAP is used.

- The password authentication protocol (PAP) transports passwords in clear text.
- The challenge handshake authentication protocol (CHAP) transports only usernames over the network. Compared with PAP, CHAP provides better security.
- With EAP relay authentication, the authenticator encapsulates 802.1x user information in the EAP attributes of RADIUS packets and sends the packets to the RADIUS server for authentication; it does not need to repackage the EAP packets into standard RADIUS packets for authentication. In this case, you can configure the **user-name-format** command but it does not take effect. Currently, the device supports these EAP modes: EAP-TLS, EAP-TTLS, EAP-MD5, and PEAP.

Note that:

- Local authentication supports only PAP and CHAP.
- For RADIUS authentication, the RADIUS server must be configured accordingly to support PAP, CHAP, or EAP authentication.

Related command: **display dot1x**.

Example # Set the 802.1x authentication method to PAP.

```
<Sysname> system-view
[Sysname] dot1x authentication-method pap
```

dot1x guest-vlan

Syntax In system view:

dot1x guest-vlan *vlan-id* [**interface** *interface-list*]

undo dot1x guest-vlan [**interface** *interface-list*]

In interface view:

dot1x guest-vlan *vlan-id*

undo dot1x guest-vlan

View System view/interface view

Parameter *vlan-id*: ID of the VLAN to be specified as the guest VLAN, in the range 1 to 4094.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x guest-vlan** command to configure the guest VLAN for specified or all ports.

Use the **undo dot1x guest-vlan** command to remove the guest VLAN(s) configured for specified or all ports.

By default, a port is configured with no guest VLAN.

In system view, this command configures guest VLAN for all ports with *interface-list* not provided, and configures guest VLAN for specified with *interface-list* provided.

In interface view, you cannot specify the *interface-list* argument and can only configure guest VLAN for the current port.

For the guest VLAN feature to take effect on a port, make sure that:

- 802.1x is enabled.
- The port access control method is set to **portbased**.
- The port access control mode is set to **auto**.
- The link type of the port is set to **access**.

Note that:

- You cannot delete a VLAN that has been configured as a guest VLAN.
- If the port access control method is set to **macbased**, the guest VLAN can be configured successfully, but the configuration does not take effect.
- You can specify a tagged VLAN as the guest VLAN for a Hybrid port, but the guest VLAN does not take effect. Similarly, if a guest VLAN for a Hybrid port is in operation, you cannot configure the guest VLAN to carry tags.
- A super VLAN cannot be set as the guest VLAN. Similarly, a guest VLAN cannot be set as the super VLAN. For information about super VLAN, refer to "VLAN Configuration Commands" on page 631.
- The guest VLAN function does not apply to non-access interfaces.

Example # Specify port Ethernet 1/0 to use VLAN999 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 999 interface ethernet 1/0
```

Specify ports Ethernet 1/2 to Ethernet 1/5 to use VLAN10 as its guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 10 interface ethernet 1/2 to ethernet 1/5
```

Specify all ports to use VLAN7 as their guest VLAN.

```
<Sysname> system-view
[Sysname] dot1x guest-vlan 7
```

Specify port Ethernet 1/7 to use VLAN3 as its guest VLAN.

```
<Sysname> system-view
[Sysname] interface ethernet 1/7
[Sysname-Ethernet1/7] dot1x guest-vlan 3
```

dot1x handshake

Syntax **dot1x handshake**

undo dot1x handshake

View Interface view

Parameter None

Description Use the **dot1x handshake** command to enable the online user handshake function so that the device can periodically send handshake messages to the client to check whether a user is online.

Use the **undo dot1x handshake** command to disable the function.

By default, the function is enabled.

Note that:

The 802.1x proxy detection function depends on the online user handshake function. Be sure to enable handshake before enabling proxy detection and to disable proxy detection before disabling handshake.

Example # Enable online user handshake.

```
<Sysname> system-view
[Sysname] interface ethernet 1/4
[Sysname-Ethernet1/4] dot1x handshake
```

dot1x max-user

Syntax In system view:

dot1x max-user *user-number* [**interface** *interface-list*]

undo dot1x max-user [**interface** *interface-list*]

In Ethernet interface view:

dot1x max-user *user-number*

undo dot1x max-user

View System view/interface view

Parameter *user-number*: Maximum number of users to be supported simultaneously. The valid settings and the default may vary by device.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x max-user** command to set the maximum number of users to be supported simultaneously for specified or all ports.

Use the **undo dot1x max-user** command to restore the default.

Note that:

- With no interface specified, the command sets the threshold for all ports when issued in system view.
- When issued in interface view, this command applies to that port only. The **interface** *interface-list* keyword and argument are not available in interface view.

Related command: **display dot1x**.

Example # Set the maximum number of users for port Ethernet 1/1 to support simultaneously as 32.

```
<Sysname> system-view
[Sysname] dot1x max-user 32 interface ethernet 1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] dot1x max-user 32
```

dot1x multicast-trigger

Syntax **dot1x multicast-trigger**

undo dot1x multicast-trigger

View Interface view

Parameter None

Description Use the **dot1x multicast-trigger** command to enable the multicast trigger function of 802.1x to send multicast trigger messages to the clients periodically.

Use the **undo dot1x multicast-trigger** command to disable this function.

By default, the multicast trigger function is enabled.

Related command: **display dot1x**.

Example # Disable the multicast trigger function for interface wlan-ess 1.

```
<Sysname> system-view
[Sysname] interface wlan-ess 1
[Sysname] undo dot1x multicast-trigger
```

dot1x port-control

Syntax In system view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** } [**interface** *interface-list*]

undo dot1x port-control [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-control { **authorized-force** | **auto** | **unauthorized-force** }

undo dot1x port-control

View System view/interface view

Parameter **authorized-force**: Places the specified or all ports in the state of authorized, allowing users of the ports to access the network without authentication.

auto: Places the specified or all ports in the state of unauthorized initially to allow only EAPOL frames to pass, and turns the ports into the state of authorized to allow access to the network after the users pass authentication. This is the most common choice.

unauthorized-force: Places the specified or all ports in the state of unauthorized, denying any access requests from users of the ports.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x port-control** command to set the access control mode for specified or all ports.

Use the **undo dot1x port-control** command to restore the default.

The default access control mode is **auto**.

Related command: **display dot1x**.

Example # Set the access control mode of port Ethernet 1/1 to **unauthorized-force**.

```
<Sysname> system-view
[Sysname] dot1x port-control unauthorized-force interface ethernet 1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] dot1x port-control unauthorized-force
```

dot1x port-method

Syntax In system view:

dot1x port-method { **macbased** | **portbased** } [**interface** *interface-list*]

undo dot1x port-method [**interface** *interface-list*]

In Ethernet interface view:

dot1x port-method { **macbased** | **portbased** }

undo dot1x port-method

View System view/interface view

Parameter **macbased**: Specifies to use the **macbased** authentication method. With this method, each user of a port must be authenticated separately, and when an authenticated user goes offline, no other users are affected.

portbased: Specifies to use the **portbased** authentication method. With this method, after the first user of a port passes authentication, all other users of the port can access the network without authentication, and when the first user goes offline, all other users get offline at the same time.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **dot1x port-method** command to set the access control method for specified or all ports.

Use the **undo dot1x port-method** command to restore the default.

The default access control method is **macbased**.

Related command: **display dot1x**.

Example # Set the access control method to **portbased** for port Ethernet 1/1.

```
<Sysname> system-view
[Sysname] dot1x port-method portbased interface ethernet 1/1
```

Or

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] dot1x port-method portbased
```

dot1x quiet-period

Syntax **dot1x quiet-period**

undo dot1x quiet-period

View System view

Parameter None

Description Use the **dot1x quiet-period** command to enable the quiet timer function.

Use the **undo dot1x quiet-period** command to disable the function.

By default, the function is disabled.

After a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in the period dictated by the quiet timer.

Related command: **display dot1x**, **dot1x timer**.

Example # Enable the quiet timer.

```
<Sysname> system-view
[Sysname] dot1x quiet-period
```

dot1x retry

Syntax **dot1x retry** *max-retry-value*

undo dot1x retry

View System view

Parameter *max-retry-value*: Maximum number of attempts to send an authentication request to a supplicant, in the range 1 to 10. The default is 2.

Description Use the **dot1x retry** command to set the maximum number of attempts to send an authentication request to a supplicant.

Use the **undo dot1x retry** command to restore the default.

By default, the authenticator can send an authentication request to a supplicant for up to twice.

Note that after sending an authentication request to a supplicant, the authenticator may retransmit the request if it does not receive any response at an interval specified by the username request timeout timer or supplicant timeout timer. The number of retransmission attempts is one less than the value set by this command.

Related command: **display dot1x**.

Example # Set the maximum number of attempts to send an authentication request to a supplicant as 9.

```
<Sysname> system-view
[Sysname] dot1x retry 9
```

dot1x supp-proxy-check

Syntax In system view:

dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

undo dot1x supp-proxy-check { **logoff** | **trap** } [**interface** *interface-list*]

In Ethernet interface view:

dot1x supp-proxy-check { **logoff** | **trap** }

undo dot1x supp-proxy-check { **logoff** | **trap** }

View System view/interface view

Parameter **logoff**: Logs off any user trying to login through a proxy.

trap: Sends a trap packet to the network management system when detecting that a user is trying to login through a proxy.

interface *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must be of the same type.

Description Use the **dot1x supp-proxy-check** command to enable detection and control of users logging in through proxies for specified or all ports.

Use the **undo dot1x supp-proxy-check** command to disable the function for specified or all ports.

By default, the function is disabled.

Note that:

- This function requires the cooperation of the 802.1x client program of H3C.
- In system view, this command enables detection and control of users' login for all ports with *interface-list* not provided, and enables detection and control of users' login for specified with *interface-list* provided.
- In interface view, you cannot specify the *interface-list* argument and can only enable detection and control of users' login for the current port.
- This function must be enabled both globally in system view and for the intended ports in system view or interface view. Otherwise, it does not work.

Related command: **display dot1x**.

Example # Specify ports Ethernet 1/1 to 1/8 to get offline users trying to login through proxies.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check logoff
[Sysname] dot1x supp-proxy-check logoff interface ethernet 1/1 to ethernet 1/8
```

Specify port Ethernet 1/9 to send a trap packet when detecting that a user is trying to login through a proxy.

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] dot1x supp-proxy-check trap interface ethernet 1/9
```

Or

```
<Sysname> system-view
[Sysname] dot1x supp-proxy-check trap
[Sysname] interface ethernet 1/9
[Sysname-Ethernet1/9] dot1x supp-proxy-check trap
```

dot1x timer

Syntax **dot1x timer** { **handshake-period** *handshake-period-value* | **quiet-period** *quiet-period-value* | **server-timeout** *server-timeout-value* | **supp-timeout** *supp-timeout-value* | **tx-period** *tx-period-value* }

undo dot1x timer { **handshake-period** | **quiet-period** | **server-timeout** | **supp-timeout** | **tx-period** }

View System view

Parameter *handshake-period-value*: Setting for the handshake timer in seconds. It ranges from 5 to 1024 and defaults to 15.

quiet-period-value: Setting for the quiet timer in seconds. It ranges from 10 to 120 and defaults to 60.

server-timeout-value: Setting for the server timeout timer in seconds. It ranges from 100 to 300 and defaults to 100.

supp-timeout-value: Setting for the supplicant timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

tx-period-value: Setting for the username request timeout timer in seconds. It ranges from 10 to 120 and defaults to 30.

Description Use the **dot1x timer** command to set 802.1x timers.

Use the **undo dot1x timer** command to restore the defaults.

Several timers are used in the 802.1x authentication process to guarantee that the supplicants, the authenticators, and the RADIUS server interact with each other in a reasonable manner. You can use this command to set these timers:

- Handshake timer (handshake-period): After a supplicant passes authentication, the authenticator sends to the supplicant handshake requests at this interval to check whether the supplicant is online. If the authenticator receives no

response after sending the allowed maximum number of handshake requests, it considers that the supplicant is offline.

- Quiet timer (quiet-period): When a supplicant fails the authentication, the authenticator refuses further authentication requests from the supplicant in this period of time.
- Server timeout timer (server-timeout): Once an authenticator sends a RADIUS Access-Request packet to the authentication server, it starts this timer. If this timer expires but it receives no response from the server, it retransmits the request.
- Supplicant timeout timer (supp-timeout): Once an authenticator sends an EAP-Request/MD5 Challenge frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request.
- Username request timeout timer (tx-period): Once an authenticator sends an EAP-Request/Identity frame to a supplicant, it starts this timer. If this timer expires but it receives no response from the supplicant, it retransmits the request. In addition, to be compatible with clients that do not send EAPOL-Start requests unsolicitedly, the device multicasts EAP-Request/Identity frame periodically to detect the clients, with the multicast interval defined by tx-period.

Generally, it is unnecessary to change the timers unless in some special or extreme network environments.

Related command: **display dot1x**.

Example # Set the server timeout timer to 150 seconds.

```
<Sysname> system-view
[Sysname] dot1x timer server-timeout 150
```

reset dot1x statistics

Syntax **reset dot1x statistics** [**interface** *interface-list*]

View User view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, which can contain multiple Ethernet ports. The *interface-list* argument is in the format of *interface-list* = { *interface-type interface-number* [**to** *interface-type interface-number*] } & <1-10>, where *interface-type* represents the port type, *interface-number* represents the port number, and & <1-10> means that you can provide up to 10 port indexes/port index lists for this argument. The start port number must be smaller than the end number and the two ports must of the same type.

Description Use the **reset dot1x statistics** command to clear 802.1x statistics.

With the **interface** *interface-list* argument specified, the command clears 802.1x statistics on the specified ports. With the argument unspecified, the command clears global 802.1x statistics and 802.1x statistics on all ports.

Related command: **display dot1x**.

Example # Clear 802.1x statistics on port Ethernet 1/1.

```
<Sysname> reset dot1x statistics interface ethernet 1/1
```

127 AAA CONFIGURATION COMMANDS

access-limit

Syntax **access-limit** { **disable** | **enable** *max-user-number* }

undo access-limit

View ISP domain view

Parameter **disable**: Specifies that the system does not limit the number of accessing users in the current ISP domain.

enable *max-user-number*: Specifies that the system limits the number of accessing users in the current ISP domain. *max-user-number* is the maximum number of accessing users in the current ISP domain. The valid range is from 1 to 1024.

Description Use the **access-limit enable** command to set the maximum number of accessing users allowed by an ISP domain.

Use the **undo access-limit** or **access-limit disable** command to remove the limitation.

By default, there is no limit to the amount of supplicants in an ISP domain.

As the supplicants may compete for network resources, setting a proper limit to the amount of accessing users helps in providing a reliable system performance.

Example # Set a limit of 500 supplicants for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] access-limit enable 500
```

accounting default

Syntax **accounting default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting default

View ISP domain view

Parameter

hwtacacs-scheme *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description

Use the **accounting default** command to specify the default accounting scheme for all types of users.

Use the **undo accounting default** command to restore the default.

By default, the accounting scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The accounting scheme specified with the **accounting default** command is for all types of users and has a priority lower than that for a specific access mode.
- Local accounting is only for managing the local user connection number; it does not provide the statistics function. The local user connection number management is only for local accounting; it does not affect local authentication and authorization.
- With the access mode of login, accounting is not supported for FTP services.

Related command:

authentication default, **authorization default**, **hwtacacs scheme**, **radius scheme**.

Example

Configure the default ISP domain **system** to use the local accounting scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] auccounting default local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for all types of users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting default radius-scheme rd local
```

Configure the default ISP domain **system** to use the default accounting scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] undo accounting default
```

accounting lan-access

Syntax **accounting lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting lan-access

View ISP domain view

Parameter **local**: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **accounting lan-access** command to specify the accounting scheme for LAN access users.

Use the **undo accounting lan-access** command to remove the accounting scheme for LAN access users.

By default, the default accounting scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **accounting default**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local accounting scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]accounting lan-access local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for LAN access users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting lan-access radius-scheme rd local
```

accounting login

Syntax **accounting login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting login

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **accounting login** command to specify the accounting scheme for login users.

Use the **undo accounting login** command to remove the accounting scheme for login users.

By default, the default accounting scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **accounting default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local accounting scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for login users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting login radius-scheme rd local
```

accounting optional

Syntax **accounting optional**

undo accounting optional

View ISP domain view

Parameter None

Description Use the **accounting optional** command to enable the accounting optional feature.

Use the **undo accounting optional** command to disable the feature.

By default, the feature is disabled.

Note that:

- With the **accounting optional** command configured, a user that will be disconnected otherwise can use the network resources even when there is no available accounting server or the communication with the current accounting server fails. This command is normally used when authentication is required but accounting is not.
- If you configure the **accounting optional** command for a domain, the device does not send real-time accounting updates or stop-accounting requests for users of the domain any more.

Example # Enable the accounting optional feature for users in domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] accounting optional
```

accounting portal

Syntax **accounting portal** { **none** | **radius-scheme** *radius-scheme-name* }

undo accounting portal

View ISP domain view

Parameter **none**: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **accounting portal** command to specify the accounting scheme for portal users.

Use the **undo accounting portal** command to restore the default.

By default, the default accounting scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **accounting default**, **radius scheme**.

Example # In the default ISP domain **system**, specify the accounting scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting portal radius-scheme rd
```

accounting ppp

Syntax **accounting ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo accounting ppp

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local accounting.

none: Does not perform any accounting.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **accounting ppp** command to specify the accounting scheme for PPP users.

Use the **undo accounting ppp** command to restore the default.

By default, the default accounting scheme is used for PPP users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **accounting default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local accounting scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting ppp local
```

Configure the default ISP domain **system** to use RADIUS accounting scheme **rd** for PPP users and to use the local accounting scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting ppp radius-scheme rd local
```

accounting voip

Syntax **accounting voip radius-scheme** *radius-scheme-name*

undo accounting voip

View ISP domain view

Parameter **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **accounting voip** command to specify the RADIUS accounting scheme for voice user.

Use the **undo accounting voip** command to restore the default.

By default, the default accounting scheme is used for VoIP users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- You must have created a RADIUS scheme before using the **accounting voip** command.
- To implement accounting, you must enable the accounting function and meanwhile have the accounting scheme configured.

Related command: **domain**, **radius scheme**

Example # In the default ISP domain **system**, configure the RADIUS accounting scheme for VoIP users to **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] accounting voip radius-scheme rd
```

attribute

Syntax **attribute** { **access-limit** *max-user-number* | **idle-cut** *minute* | **ip** *ip-address* | **location** { [**nas-ip** *ip-address* **port** *slot-number subslot-number port-number* |] **port** *slot-number subslot-number port-number* } | **mac** *mac-address* | **vlan** *vlan-id* } *

undo attribute { **access-limit** | **idle-cut** | **ip** | **location** | **mac** |**vlan** }*

View Local user view

Parameter **access-limit** *max-user-number*: Specifies the maximum number of concurrent users that can log in using the current username, which ranges from 1 to 1024.

idle-cut *minute*: Configures the idle cut function. The idle cut period ranges from 1 to 120, in minutes.

ip *ip-address*: Specifies the IP address of the user. The **attribute ip** command only applies to authentications that support IP address passing, such as 802.1x. If you configure the command to authentications that do not support IP address passing, such as MAC address authentication, the local authentication will fail.

location: Specifies the port binding attribute of the user.

nas-ip *ip-address*: Specifies the IP address of the port of the remote access server bound by the user. The default is 127.0.0.1, that is, the device itself. This keyword and argument combination is required only when the user is bound to a remote port.

port *slot-number subslot-number port-number*: Specifies the port to which the user is bound. The value of *slot-number* and *subslot-number* both range from 0 to 15. The value of *port-number* ranges from 0 to 255. The ports bounded are determined by port number, regardless of port type.

mac *mac-address*: Specifies the MAC address of the user in the format of *H-H-H.*

vlan *vlan-id*: Specifies the VLAN to which the user belongs. The *vlan-id* argument is in the range 1 to 4094.

Description Use the **attribute** command to set some of the attributes for a LAN access user.

Use the **undo attribute** command to remove the configuration.

The **idle-cut** command in user interface view applies to lan-access users only.

Related command: **display local-user**.

Example # Set the IP address of local user **user1** to 10.110.50.1.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] attribute ip 10.110.50.1
```

authentication default

Syntax **authentication default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication default

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication default** command to specify the default authentication scheme for all types of users.

Use the **undo authentication default** command to restore the default.

By default, the authentication scheme is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.
- The authentication scheme specified with the **authentication default** command is for all types of users and has a priority lower than that for a specific access mode.

Related command: **authorization default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authentication scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for all types of users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication default radius-scheme rd local
```

authentication lan-access

Syntax **authentication lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication lan-access

View ISP domain view

Parameter **local**: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication lan-access** command to specify the authentication scheme for LAN access users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **authentication default**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authentication scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for LAN access users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication lan-access radius-scheme rd local
```

authentication login

Syntax **authentication login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication login

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication login** command to specify the authentication scheme for login users.

Use the **undo authentication login** command to restore the default.

By default, the default authentication scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **authentication default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authentication scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for login users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication login radius-scheme rd local
```

authentication portal

Syntax **authentication portal** { **none** | **radius-scheme** *radius-scheme-name* }

undo authentication portal

View ISP domain view

Parameter **none**: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication portal** command to specify the authentication scheme for portal users.

Use the **undo authentication portal** command to restore the default.

By default, the default authentication scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **authentication default**, **radius scheme**.

Example # In the default ISP domain **system**, specify the authentication scheme for portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication portal radius-scheme rd
```

authentication ppp

Syntax **authentication ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authentication ppp

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authentication.

none: Does not perform any authentication.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication ppp** command to specify the authentication scheme for PPP users.

Use the **undo authentication ppp** command to restore the default.

By default, the default authentication scheme is used for PPP users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **authentication default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authentication scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication ppp local
```

Configure the default ISP domain **system** to use RADIUS authentication scheme **rd** for PPP users and to use the local authentication scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication ppp radius-scheme rd local
```

authentication voip

Syntax **authentication voip radius-scheme** *radius-scheme-name*

undo authentication voip

View ISP domain view

Parameter **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authentication voip** command to specify the authentication RADIUS scheme for VoIP users.

Use the **undo authentication voip** command to restore the default.

By default, the default authentication scheme is used for VoIP users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- You must have created a RADIUS scheme before using the **authentication voip** command.
- To implement authentication, you must enable the authentication function and meanwhile have the authentication scheme configured.

Related command: **domain**, **radius scheme**.

Example # In the default ISP domain **system**, configure the RADIUS authentication scheme for VoIP users to **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authentication voip radius-scheme rd
```

authorization command

Syntax **authorization command hwtacacs-scheme** *hwtacacs-scheme-name*

undo authorization command

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization command** command to specify the authorization scheme for command line users.

Use the **undo authorization command** command to restore the default.

By default, the default authorization scheme is used for command line users.

Note that the HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **authorization default**, **hwtacacs scheme**.

Example # Configure the default ISP domain **system** to use HWTACACS authorization scheme hw for command line users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization command hwtacacs-scheme hw
```

authorization default

Syntax **authorization default** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization default

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization default** command to specify the authorization scheme for all types of users.

Use the **undo authorization default** command to restore the default.

By default, the authorization scheme for all types of users is **local**.

Note that:

- The RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

- The authorization scheme specified with the **authorization default** command is for all types of users and has a priority lower than that for a specific access mode.
- RADIUS authorization is special in that it takes effect only when the RADIUS authorization scheme is the same as the RADIUS authentication scheme. In addition, if a RADIUS authorization fails, the error message returned to the NAS says that the server is not responding.

Related command: **authentication default**, **accounting default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authorization scheme for all types of users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for all types of users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization default radius-scheme rd local
```

authorization lan-access

Syntax **authorization lan-access** { **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization lan-access

View ISP domain view

Parameter **local**: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization lan-access** command to specify the authorization scheme for LAN access users.

Use the **undo authorization lan-access** command to restore the default.

By default, the default authorization scheme is used for LAN access users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **authorization default**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authorization scheme for LAN access users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization lan-access local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for LAN access users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization lan-access radius-scheme rd local
```

authorization login

Syntax **authorization login** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization login

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization login** command to specify the authorization scheme for login users.

Use the **undo authorization login** command to restore the default.

By default, the default authorization scheme is used for login users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **authorization default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authorization scheme for login users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for login users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization login radius-scheme rd local
```

authorization portal

Syntax **authorization portal** { **none** | **radius-scheme** *radius-scheme-name* }

undo authorization portal

View ISP domain view

Parameter **none**: None authorization, which means the user is trusted completely. Here, the user is assigned with the default privilege.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization portal** command to specify the authorization scheme for portal users.

Use the **undo authorization portal** command to restore the default.

By default, the default authorization scheme is used for portal users.

Note that the RADIUS scheme specified for the current ISP domain must have been configured.

Related command: **authorization default**, **radius scheme**.

Example # In the default ISP domain **system**, specify the authorization scheme for Portal users to RADIUS scheme, with the name **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization portal radius-scheme rd
```

authorization ppp

Syntax **authorization ppp** { **hwtacacs-scheme** *hwtacacs-scheme-name* [**local**] | **local** | **none** | **radius-scheme** *radius-scheme-name* [**local**] }

undo authorization ppp

View ISP domain view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies an HWTACACS scheme by its name, which is a string of 1 to 32 characters.

local: Performs local authorization.

none: Does not perform any authorization. In this case, an authenticated user is automatically authorized with the default right.

radius-scheme *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization ppp** command to specify the authorization scheme for PPP users.

Use the **undo authorization ppp** command to restore the default.

By default, the default authorization scheme is used for PPP users.

Note that the RADIUS or HWTACACS scheme specified for the current ISP domain must have been configured.

Related command: **authorization default**, **hwtacacs scheme**, **radius scheme**.

Example # Configure the default ISP domain **system** to use the local authorization scheme for PPP users.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system]authorization ppp local
```

Configure the default ISP domain **system** to use RADIUS authorization scheme **rd** for PPP users and to use the local authorization scheme as the backup scheme.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization ppp radius-scheme rd local
```

authorization voip

Syntax **authorization voip radius-scheme** *radius-scheme-name*

undo authorization voip

View ISP domain view

Parameter **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

Description Use the **authorization voip** command to specify the authorization scheme for VoIP users.

Use the **undo authorization voip** command to restore the default.

By default, the default authorization scheme configured is used for VoIP users.

Note that:

- The RADIUS scheme specified for the current ISP domain must have been configured.
- You must have created a RADIUS scheme before using the **authorization voip** command.
- The scheme specified in this command must be the same with authentication scheme, otherwise authorization will fail.
- To implement authorization, you must enable the authorization function and meanwhile have the authorization scheme configured.

Related command: **domain**, **radius scheme**

Example # In the default ISP domain **system**, configure the RADIUS authorization scheme for voice users to **rd**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] authorization voip radius-scheme rd
```

cut connection

Syntax **cut connection** { **access-type** { **dot1x** | **mac-authentication** | **portal** } | **all** | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id* }

View System view

Parameter **access-type**: Specifies user connections of an access mode.

- **dot1x**: Specifies 802.1x authentication user connections.
- **mac-authentication**: Specifies MAC authentication user connections.
- **portal**: Specifies portal authentication user connections.

all: Specifies all user connections.

domain *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies all user connections of an interface. Currently, the *interface-type* argument can be only Layer 2 Ethernet interface and Layer 2 WLAN virtual interface.

ip *ip-address*: Specifies a user connection by IP address.

mac *mac-address*: Specifies a user connection by MAC address. The MAC address must be in the format of *H-H-H.*

user-name *user-name*: Specifies a user connection by username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. The system assumes that a username entered contains the domain name.

ucibindex *ucib-index*: Specifies a user connection by connection index. The value range varies by device.

vlan *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

Description Use the **cut connection** command to tear down the specified connections forcibly.

This command is effective to LAN-access, portal, and PPP user connections only.

Related command: **display connection**, **service-type**

Example # Tear down all connections in ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] cut connection domain aabbcc.net
```

display connection

Syntax **display connection** [**access-type** { **dot1x** | **mac-authentication** | **portal** } | **domain** *isp-name* | **interface** *interface-type interface-number* | **ip** *ip-address* | **mac** *mac-address* | **ucibindex** *ucib-index* | **user-name** *user-name* | **vlan** *vlan-id*]

View Any view

Parameter **access-type** { **dot1x** | **mac-authentication** | **portal** }: Specifies user connections of an access mode, that is, 802.1x user connections, MAC authentication user connections, or portal authentication user connections.

domain *isp-name*: Specifies all user connections of an ISP domain. The *isp-name* argument refers to the name of an existing ISP domain and is a case-insensitive string of 1 to 24 characters.

interface *interface-type interface-number*: Specifies all user connections of an interface.

ip *ip-address*: Specifies all user connections using the specified IP address.

mac *mac-address*: Specifies all user connections using the specified MAC address. The MAC address must be in the format of *H-H-H.*

ucibindex *ucib-index*: Specifies all user connections using the specified connection index. The valid range of the *ucib-index* argument varies by device.

user-name *user-name*: Specifies all user connections using the specified username. The *user-name* argument is a case-sensitive string of 1 to 80 characters and must contain the domain name. The system assumes that a username entered contains the domain name.

vlan *vlan-id*: Specifies all user connections in a VLAN. The VLAN ID ranges from 1 to 4094.

Description Use the **display connection** command to display information about specified or all AAA user connections.

- *If no argument is specified, this command displays information about all AAA user connections.*
- *This command does not apply to FTP user connections.*

Related command: **cut connection**.

Example # Display information about all AAA user connections.

```
<Sysname> display connection

Index=1    ,Username=telnet@system
IP=10.0.0.1
 Total 1 connection(s) matched.
```

Table 507 Description on the fields of the display connection command

Field	Description
Index	Index number
Username	Username of the connection, in the format *username@domain*
IP	IP address of the user
Total 1 connection(s) matched.	Total number of user connections

display domain

Syntax **display domain** [*isp-name*]

View Any view

Parameter *isp-name*: Name of an existing ISP domain, a case-insensitive string of 1 to 24 characters.

Description Use the **display domain** command to display the configuration information of a specified ISP domain or all ISP domains.

Related command: **access-limit**, **domain**, **state**.

Example # Display the configuration information of all ISP domains.

```
<Sysname> display domain
0  Domain = aabbcc
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Lan-access authentication scheme     radius=test, local
   Lan-access authorization scheme      hwtacacs=hw, local
   Lan-access accounting scheme       : local
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable

1  Domain = system
   State = Active
   Access-limit = Disable
   Accounting method = Required
   Default authentication scheme      : local
   Default authorization scheme       : local
   Default accounting scheme          : local
   Login Accounting scheme            : none
   Domain User Template:
   Idle-cut = Disable
   Self-service = Disable

Default Domain Name: system
Total 2 domain(s) 2 listed.
```

Table 508 Description on the fields of the display domain command

Field	Description
Domain	Domain name
State	Status of the domain (active or block)
Access-limit	Access limit (disabled or enabled)
Accounting method	Accounting method (either required or optional)
Default authentication scheme	Default authentication scheme
Default authorization scheme	Default authorization scheme
Default accounting scheme	Default accounting scheme
Authentication scheme	Authentication scheme
Authorization scheme	Authentication scheme
Accounting scheme	Accounting scheme

Table 508 Description on the fields of the display domain command

Field	Description
Domain User Template	Template for users in the domain
Idle-cut	Whether idle cut is enabled
Self-service	Whether self service is enabled
Total 2 domain(s).	2 ISP domains in total

display local-user

Syntax **display local-user** [**idle-cut** { **disable** | **enable** } | **service-type** { **dvpn** | **ftp** | **lan-access** | **pad** | **ppp** | **ssh** | **telnet** | **terminal** } | **state** { **active** | **block** } | **user-name** *user-name* | **vlan** *vlan-id*]

View Any view

Parameter **idle-cut** { **disable** | **enable** }: Specifies local users with the idle cut function disabled or enabled.

service-type: Specifies the local users of a type.

- **dvpn** refers to users using DVPN tunnel,
- **ftp** refers to users using FTP,
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1x users,
- **pad** refers to users using x.25 PAD,
- **ppp** refers to users using PPP,
- **ssh** refers to users using SSH,
- **telnet** refers to users using Telnet,
- **terminal** refers to users logging in through the console port, AUX port, or Asyn port.

state { **active** | **block** }: Specifies all local users in the state of active or block. A local user in the state of active can access network services, while a local user in the state of blocked cannot.

user-name *user-name*: Specifies all local users using the specified username. The username is a case-sensitive string of 1 to 55 characters and does not contain the domain name.

vlan *vlan-id*: Specifies all local users in a VLAN. The VLAN ID ranges from 1 to 4094.

Description Use the **display local-user** command to display information about specified or all local users.

Related command: **local-user**.

Example # Display information about all local users.

```
<Sysname> display local-user
The contents of local user abc:
 State:                    Active
 ServiceType:              ftp
 Idle-cut:                 Disable
 Access-limit:             Enable            Current AccessNum: 0
 Bind location:            2.2.2.2/3/2/255 (NAS/SLOT/SUBSLOT/PORT)
 Vlan ID:                  Disable
 IP address:               Disable
 MAC address:              Disable
 Password-Aging:           Enable(90 day(s))
 Password-Length:          Enable(10 character(s))
 Password-Composition:     Enable(1 type(s),  1 character(s) per type)
Total 1 local user(s) matched
```

Table 509 Description on the fields of display local-user

Field	Description
State	Status of the local user: active or block
ServiceType	Service types that the user can use (ftp, lan-access, pad, ssh, telnet, terminal)
Idle-cut	Whether idle cut is enabled
Access-limit	Accessing user connection limit
Current AccessNum	Number of users currently accessing network services
Bind location	Whether bound with a port
VLAN ID	VLAN to which the user belongs
IP address	IP address of the user
MAC address	MAC address of the user
Password-Aging	Aging time of the local user password
Password-Length	Minimum length of the local user password
Password-Composition	Password composition policy of the local user
Total 1 local user(s) matched	1 local user in total

domain

Syntax **domain** *isp-name*

undo domain *isp-name*

View System view

Parameter *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or at-sign (@).

Description Use the **domain** *isp-name* command to create an ISP domain and/or enter ISP domain view.

Use the **domain default** command to specify the default ISP domain and enter ISP domain view.

Use the **undo domain** command to remove an ISP domain.

By default, the system uses the domain of system. You can view its settings by executing the **display domain** command.

If the specified ISP domain does not exist, the system will create a new ISP domain. All the ISP domains are in the active state when they are created.

Related command: **access-limit**, **state**, **display domain**.

Example # Create ISP domain **aabbcc.net**, and enter ISP domain view.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net]
```

domain default

Syntax **domain default** { **disable** | **enable** *isp-name* }

View System view

Parameter **disable:** disables the configured default ISP domain.

enable: Enables the configured default ISP domain.

isp-name: Name of an existing ISP domain, a case-insensitive string of 1 to 24 characters.

Description Use the **domain default** command to manually configure the system default ISP domain.

By default, the default domain is named system.

Note that:

- There must be only one default ISP domain.
- When configure a default domain, this domain must have existed.
- The default domain configured cannot be deleted unless you cancel it as a default domain first.

Related command: **state**, **display domain**.

Example # Create a new ISP domain named **aabbcc.net**, and configure it as the default ISP domain.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] quit
[Sysname] domain default enable aabbcc.net
```

idle-cut

Syntax **idle-cut** { **disable** | **enable** *minute* }

View ISP domain view

Parameter **disable**: Disables the idle cut function.

enable *minute*: Enables the idle cut function. The *minute* argument refers to the allowed idle duration, in the range 1 to 120 minutes.

Description Use the **idle-cut** command to enable or disable the idle cut function.

By default, the function is disabled.

Related command: **domain**.

Example # Enable the idle cut function and set the idle threshold to 50 minutes for ISP domain **aabbcc.net**.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] idle-cut enable 50
```

ip pool

Syntax **ip pool** *pool-number low-ip-address* [*high-ip-address*]

undo ip pool *pool-number*

View System view, ISP domain view

Parameter *pool-number*: Address pool number, in the range 0 to 99.

low-ip-address and *high-ip-address*: Start and end IP addresses of the address pool. Up to 1024 addresses are allowed for an address pool. If you do not specify the end IP address, there will be only one IP address in the pool, namely the start IP address.

Description Use the **ip pool** command to configure an address pool for assigning addresses to PPP users.

Use the **undo ip pool** command to delete an address pool.

By default, no IP address pool is configured for PPP users.

- Configure an IP address pool in system view and use the **remote address** command in interface view to assign IP addresses from the pool to PPP users.

- You can also configure an IP address pool in ISP domain view for assigning IP addresses to the PPP users in the ISP domain. This applies to the scenario where an interface serves a great amount of PPP users but the address resources are inadequate. For example, an Ethernet interface running PPPoE can accommodate up to 4095 users. However, only one address pool with up to 1024 addresses can be configured on its virtual template (VT). This is obviously far from what is required. To address the issue, you can configure address pools for ISP domains and assign addresses from them to the PPP users by domain.

Related command: **remote address** on page 523.

Example # Configure the IP address pool 0 with the address range of 129.102.0.1 to 129.102.0.10.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] ip pool 0 129.102.0.1 129.102.0.10
```

level

Syntax **level** *level*

undo level

View Local user view

Parameter *level*: Priority level for the user, which can be 0 for visiting level, 1 for monitoring level, 2 for system level, and 3 for administration level. A smaller number means a lower priority.

Description Use the **level** command to set the priority level of a user.

Use the **undo level** command to restore the default.

By default, the user priority is 0.

Note that:

- If you specify not to perform authentication or use password authentication, the level of the commands that a user can use after logging in depends on the priority of the user interface. For details about the authentication, refer to *"authentication-mode" on page 2452.*
- If you specify an authentication method that requires the username and password, the level of the commands that a user can use after logging in depends on the priority of the user. For an SSH user using RSA public key authentication, the commands that can be used depend on the level configured on the user interface.

Related command: **local-user**.

Example # Set the level of user **user1** to 3.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] level 3
```

local-user

Syntax **local-user** *user-name*

undo local-user { *user-name* | **all** [**service-type** { **dvpn** | **ftp** | **lan-access** | **pad** | **ppp** | **ssh** | **telnet** | **terminal** } }

View System view

Parameter *user-name*: Name for the local user, a case-sensitive string of 1 to 55 characters that does not contain the domain name. It cannot contain any backward slash (\), forward slash (/), vertical line (|), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>) and the @ sign and cannot be a, al, or all.

all: Specifies all users.

service-type: Specifies the users of a type.

- **dvpn** refers to users using DVPN tunnel,
- **ftp** refers to users using FTP,
- **lan-access** refers to users accessing the network through an Ethernet, such as 802.1x users,
- **pad** refers to users using x.25 PAD,
- **ppp** refers to users using PPP,
- **ssh** refers to users using SSH,
- **telnet** refers to users using Telnet,
- **terminal** refers to users logging in through the console port, AUX port, or Asyn port.

Description Use the **local-user** command to add a local user and enter local user view.

Use the **undo local-user** command to remove the specified local users.

By default, no local user is configured.

Related command: **display local-user**, **service-type**.

Example # Add a local user named **user1**.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1]
```

local-user password-display-mode

Syntax **local-user password-display-mode** { **auto** | **cipher-force** }

undo local-user password-display-mode

View System view

Parameter **auto**: Displays the password of an accessing user based on the configuration of the user by using the **password** command.

cipher-force: Displays the passwords of all accessing users in cipher text.

Description Use the **local-user password-display-mode** command to set the password display mode for all local users.

Use the **undo local-user password-display-mode** command to restore the default.

The default mode is **auto**.

With the **cipher-force** mode configured,

- A local user password is always displayed in cipher text, regardless of the configuration of the **password** command.
- If you use the **save** command to save the configuration, all existing local user passwords will still be displayed in cipher text after the device restarts, even if you restore the display mode to **auto**.

Related command: **display local-user**, **password**.

Example # Specify to display the passwords of all accessing users in cipher text.

```
[Sysname] local-user password-display-mode cipher-force
```

password

Syntax **password** { **cipher** | **simple** } *password*

undo password

View Local user view

Parameter **cipher**: Specifies to display the password in cipher text.

simple: Specifies to display the password in simple text.

password: Password for the local user.

- In simple text, it must be a string of 1 to 63 characters that contains no blank space, for example, aabbcc.
- In cipher text, it must be a string of 24 or 88 characters, for example, _(TT8F]Y5SQ=^Q‘MAF4<1!!.
- With the **simple** keyword, you must specify the password in simple text. With the **cipher** keyword, you can specify the password in either simple or cipher text.

Description Use the **password** command to configure a password for a local user.

Use the **undo password** command to delete the password of a local user.

Note that:

- With the **local-user password-display-mode cipher-force** command configured, the password is always displayed in cipher text, regardless of the configuration of the **password** command.
- With the **cipher** keyword specified, a password of up to 16 characters in plain text will be encrypted into a password of 24 characters in cipher text, and a password of 16 to 63 characters in plain text will be encrypted into a password of 88 characters in cipher text. For a password of 24 characters, if the system can decrypt the password, the system treats it as a password in cipher text. Otherwise, the system treats it as a password in plain text.

Related command: **display local-user**.

Example # Set the password of **user1** to **123456** and specify to display the password in plain text.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] password simple 123456
```

self-service-url

Syntax **self-service-url** { **disable** | **enable** *url-string* }

undo self-service-url

View ISP domain view

Parameter **disable**: Disables the self-service server localization function.

enable *url-string*: Enables the self-service server localization function. The *url-string* argument refers to the URL of the self-service server for changing user password. The URL is a string of 1 to 64 characters that starts with http:// and cannot contain any question mark.

Description Use the **self-service-url enable** command to enable the self-service server localization function and specify the URL of the self-service server for changing user password.

Use the **self-service-url disable** command or the **undo self-service-url** command to disable the self-service server localization function.

By default, the function is disabled.

Note that:

- A self-service RADIUS server, for example, CAMS, is required for the self-service server localization function. With the self-service function, a user can manage and control his or her accounting information or card number. A server with self-service software is a self-service server.
- After you configure the **self-service-url enable** command, a user can locate the self-service server by selecting [Service/Change Password] from the 802.1x client. The client software automatically launches the default browser, IE or Netscape, and opens the URL page of the self-service server for changing the user password. A user can change his or her password through the page.
- Only authenticated users can select [Service/Change Password] from the 802.1x client. The option is gray and unavailable for unauthenticated users.

Example # Enable the self-service server localization function and specify the URL of the self-service server for changing user password to http://10.153.89.94/selfservice/modPasswd1x.jsp|userName for the default ISP domain **system**.

```
<Sysname> system-view
[Sysname] domain system
[Sysname-isp-system] self-service-url enable http://10.153.89.94/sel
fservice/modPasswd1x.jsp|userName
```

service-type

Syntax **service-type** { **lan-access** | { **dvpn** | **pad** | **ssh** | **telnet** | **terminal** }* [**level** *level*] }

undo service-type { **lan-access** | { **pad** | **ssh** | **telnet** | **terminal** }* }

View Local user view

Parameter **lan-access**: Authorizes the user to use the Ethernet to access the network. The user can be, for example, an 802.1x user.

dvpn: Authorizes the user to use the DVPN service.

pad: Authorizes the user to use the PAD service.

ssh: Authorizes the user to use the SSH service.

telnet: Authorizes the user to use the Telnet service.

terminal: Authorizes the user to use the terminal service, allowing the user to login from the console, AUX or Asyn port.

level *level*: Sets the user level of a Telnet, terminal, or SSH user. The *level* argument is an integer in the range 0 to 3 and defaults to 0.

Description Use the **service-type** command to specify the service types that a user can use.

Use the **undo service-type** command to delete one or all service types configured for a user.

By default, a user is authorized with no service.

Related command: **service-type ppp** and **service-type ftp**.

Example # Authorize user **user1** to use the Telnet service.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type telnet
```

service-type ftp

Syntax **service-type ftp**

undo service-type ftp

View Local user view

Parameter None

Description Use the **service-type ftp** command to authorize a user to use the FTP service.

Use the **undo service-type ftp** command to disable a user from using the FTP service.

By default, no service is authorized to a user and anonymous access to FTP service is not allowed. If you authorize a user to use the FTP service, the user can access the root directory of the device by default.

Related command: **work-directory**, **service-type**, **service-type ppp**.

Example # Authorize user **user1** to use the FTP service.

```
[Sysname-luser-user1] service-type ftp
```

service-type ppp

Syntax **service-type ppp** [**call-number** *call-number* [**:** *subcall-number*] | **callback-nocheck** | **callback-number** *callback-number*]

undo service-type ppp [**call-number** | **callback-nocheck** | **callback-number**]

View Local user view

Parameter **call-number** *call-number*: Specifies a caller number for ISDN user authentication, which is a string of 1 to 64 characters.

[: *subcall-number*]: Specifies the sub-caller number. The total length of the caller number and the sub-caller number must be less than 62 characters.

callback-nocheck: Enables the PPP user callback without authentication feature.

callback-number *callback-number*: Specifies a callback number, which is a string of 1 to 64 characters.

Description Use the **service-type ppp** command to authorize a user to use the PPP service and configure the callback attribute and caller number of the user.

Use the **undo service-type ppp** command to restore their default settings.

By default, no service is authorized to a user; if the PPP service is authorized, callback without authentication is enabled, no callback number is specified, and the system does not authenticate the caller number of ISDN users.

Related command: **service-type** and **service-type ftp**.

Example # Authorize user **user1** to use the PPP service and enable the callback without authentication feature.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] service-type ppp callback-nocheck
```

state

Syntax **state** { **active** | **block** }

View ISP domain view/local user view

Parameter **active**: Places the current ISP domain or local user in the active state, allowing the users in the current ISP domain or the current local user to request network services.

block: Places the current ISP domain or local user in the blocked state, preventing users in the current ISP domain or the current local user from requesting network services.

Description Use the **state** command to configure the status of the current ISP domain or local user.

By default, an ISP domain is active when created. So does a local user.

By blocking an ISP domain, you disable users of the domain that are offline from requesting network services. Note that the online users are not affected.

By blocking a user, you disable the user from requesting network services. No other users are affected.

Related command: **domain**.

Example # Place the current ISP domain **aabbcc.net** to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-isp-aabbcc.net] state block
```

Place the current user **user1** to the state of blocked.

```
<Sysname> system-view
[Sysname] domain aabbcc.net
[Sysname-user-user1] state block
```

work-directory

Syntax **work-directory** *directory-name*

undo work-directory

View Local user view

Parameters *directory-name*: Name of the directory that FTP/SFTP users are authorized to access, a case-insensitive string of 1 to 135 characters.

Description Use the **work-directory** command to specify the directory accessible to FTP/SFTP users.

Use the **undo work-directory** command to restore the default.

By default, FTP/SFTP users can access the root directory of the device.

Note that:

- The specified directory accessible to users must exist.
- If you use a file system command to delete the specified directory, FTP/SFTP users will no longer access the directory.
- If the specified directory carries with information about the slot where the secondary board is inserted, FTP/SFTP users cannot log in after primary-to-secondary switching. It is not recommended to carry with slot information when you specify a work directory.

Example # Specify the directory accessible to FTP/SFTP users.

```
<Sysname> system-view
[Sysname] local-user user1
[Sysname-luser-user1] work-directory cf:
```

128 RADIUS CONFIGURATION COMMANDS

accounting-on enable

Syntax **accounting-on enable**

undo accounting-on enable

View RADIUS scheme view

Parameter None

Description Use the **accounting-on enable** command to enable the accounting-on function. After doing so, when the device reboots, a message will be sent to the RADIUS server to force the users of the device offline.

Use the **undo accounting-on enable** command to disable the accounting-on function.

By default, the accounting-on function is disabled.

Note that:

- This command is applicable to centralized devices only.
- Execution of this command does not affect the results of other accounting-on related commands such as **accounting-on enable send**.
- If the system has no authentication scheme enabled with the accounting-on function when you execute the **accounting-on enable** command, you need to save the configuration and restart the device so that the command takes effect. Otherwise, the command takes effect immediately.

Related command: **radius scheme**.

Example # Enable the accounting-on function for RADIUS authentication scheme **rd**.

```
<Sysname> system-view
[Sysname] radius scheme rd
[Sysname-radius-rd] accounting-on enable
```

accounting-on enable interval

Syntax **accounting-on enable interval** *seconds*

undo accounting-on interval

View RADIUS scheme view

Parameter *seconds*: Time interval to retransmit accounting-on packet in seconds, ranging from 1 to 15.

Description Use the **accounting-on enable interval** command to configure the retransmission interval of accounting-on packets.

Use the **undo accounting-on enable interval** command to restore the default.

By default, the retransmission interval of accounting-on packets is 3 seconds.

Note that:

- This command is applicable to centralized devices only.
- Execution of this command does not affect the results of other accounting-on related commands such as **accounting-on enable**. That is, execution of the **undo accounting-on enable interval** command will not disable the accounting-on function.
- The retransmission interval configured with this command takes effect immediately.

Related command: **radius scheme**, **accounting-on enable**

Example # In RADIUS scheme **rd**, set the retransmission interval of accounting-on packet to 5 seconds.

```
<Sysname> system-view
[Sysname] radius scheme rd
[Sysname-radius-rd] accounting-on enable interval 5
```

accounting-on enable send

Syntax **accounting-on enable send** *send-times*

undo accounting-on send

View RADIUS scheme view

Parameter *send-times*: Maximum number of accounting-on packet retransmission attempts, ranging from 1 to 255.

Description Use the **accounting-on enable send** command to set the maximum number of accounting-on packet retransmission attempts.

Use the **undo accounting-on enable send** command to restore the default.

By default, the maximum number of accounting-on packet retransmission attempts is 5.

Note that:

- This command is applicable to centralized devices only.
- Execution of this command does not affect the results of other accounting-on related commands such as **accounting-on enable**. That is, execution of the **undo accounting-on enable interval** command will not disable the accounting-on function.
- The maximum number of accounting-on packet retransmission attempts configured with this command takes effect immediately.

Related command: **radius scheme**, **accounting-on enable**.

Example # In RADIUS scheme **rd**, set the maximum number of accounting-on packet retransmission attempts to 10.

```
<Sysname> system-view
[Sysname] radius scheme rd
[Sysname-radius-rd] accounting-on enable send 10
```

data-flow-format (RADIUS scheme view)

Syntax **data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*

undo data-flow-format { **data** | **packet** }

View RADIUS scheme view

Parameter **data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a RADIUS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Related command: **display radius scheme**.

Example # Define RADIUS scheme **radius1** to send data flows and packets destined for the RADIUS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] data-flow-format data kilo-byte packet kilo-packet
```

display radius scheme

Syntax **display radius scheme** [*radius-scheme-name*]

View Any view

Parameter *radius-scheme-name*: RADIUS scheme name.

Description Use the **display radius scheme** command to display the configuration information of a specified RADIUS scheme or all RADIUS schemes.

Related command: **radius scheme**.

Example # Display the configurations of all RADIUS schemes.

```
<Sysname> display radius scheme
------------------------------------------------------------------
  SchemeName  = systemradius1
  Index=0                          Type=extended
  Primary Auth IP  =127.0.0. 1.1.1.1          Port=1645 = 1812   State=block
 = active
  Primary Acct IP  =127.0.0.1 1.1.1.1          Port=1646 = 1813   State=bloc
k = active
  Second  Auth IP  = 0.0.0.0          Port= = 1812   State= = block
  Second  Acct IP  = 0.0.0.0          Port= = 1813   State= = block
  Auth Server Encryption Key= Not configured
  Acct Server Encryption Key= Not configured
  Accounting-On packet disable, send times = 5 , interval = 3s
  Interval for timeout(second)                          =3
  Retransmission times for timeout                      =3
  Interval for realtime accounting(minute)              =12
  Retransmission times of realtime-accounting packet    =5
  Retransmission times of stop-accounting packet        =500
  Quiet-interval(min)                                   =5
  Username format                                       =without-domain
  Data flow unit                                        =Byte
  Packet unit                                           =one

------------------------------------------------------------------
Total 1 RADIUS scheme(s)
```

Table 510 Description on the fields of the display radius scheme command

Field	Description
SchemeName	Name of the RADIUS scheme
Index	Index number of the RADIUS scheme
Type	Type of the RADIUS server

Table 510 Description on the fields of the display radius scheme command

Field	Description
Primary Auth IP/ Port/ State	IP address/access port number/current status of the primary authentication server: (active or block)
Primary Acct IP/ Port/ State	IP address/access port number/current status of the primary accounting server: (active or block)
Second Auth IP/ Port/ State	IP address/access port number/current status of the secondary authentication server: (active or block)
Second Acct IP/ Port/ State	IP address/access port number/current status of the secondary accounting server: (active or block)
Auth Server Encryption Key	Shared key of the authentication server
Acct Server Encryption Key	Shared key of the accounting server
Accounting-On packet disable	The accounting-on function is disabled
send times	Retransmission times of accounting-on packets
interval	Interval to retransmit accounting-on packets
Interval for timeout(second)	Timeout time in seconds
Retransmission times for timeout	Times of retransmission in case of timeout
Interval for realtime accounting(minute)	Interval for realtime accounting in minutes
Retransmission times of realtime-accounting packet	Retransmission times of realtime-accounting packet
Retransmission times of stop-accounting packet	Retransmission times of stop-accounting packet
Quiet-interval(min)	Quiet interval for the primary server
Username format	Format of the username
Data flow unit	Unit of data flows
Packet unit	Unit of packets
Total 1 RADIUS scheme(s)	1 RADIUS scheme in total

display radius statistics

Syntax **display radius statistics**

View Any view

Parameter None

Description Use the **display radius statistics** command to display statistics about RADIUS packets.

Related command: **radius scheme**.

Example # Display statistics about RADIUS packets.

```
<Sysname> display radius statistics
state statistic(total=1024):
     DEAD= = 1024     AuthProc= = 0        AuthSucc= = 0
AcctStart= = 0         RLTSend= = 0         RLTWait= = 0
```

```
 AcctStop= = 0          OnLine= = 0            Stop= = 0

Received and Sent packets statistic:
Sent PKT total  : = 0        Received PKT total: = 0
RADIUS received packets statistic:
Resend Times     Resend total
1                0
2                0
Total            0
Running statistic:
RADIUS received messages statistic:
Normal auth request             , Num= = 0       , Err= = 0       ,
Succ= = 0
EAP auth request                , Num= = 0       , Err= = 0       ,
Succ= = 0
Account request                 , Num= = 0       , Err= = 0       ,
Succ= = 0
Account off request             , Num= = 0       , Err= = 0       ,
Succ= = 0
PKT auth timeout                , Num= = 0       , Err= = 0       ,
Succ= = 0
PKT acct_timeout                , Num= = 0       , Err= = 0       ,
Succ= = 0
Realtime Account timer          , Num= = 0       , Err= = 0       ,
Succ= = 0
PKT response                    , Num= = 0       , Err= = 0       ,
Succ= = 0
Session ctrl pkt                , Num= = 0       , Err= = 0       ,
Succ= = 0
Normal author request           , Num= = 0       , Err= = 0       ,
Succ= = 0
RADIUS sent messages statistic:
Auth accept                     , Num= = 0
Auth reject                     , Num= = 0
EAP auth replying               , Num= = 0
Account success                 , Num=0
Account failure                 , Num=0
Server ctrl req                 , Num=0
RecError_MSG_sum:0        SndMSG_Fail_sum :0
Timer_Err       :0        Alloc_Mem_Err   :0
State Mismatch  :0        Other_Error     : = 0

Account failure          Num = 0
Server ctrl req          Num = 0
RecError_MSG_sum = 0
SndMSG_Fail_sum  = 0
Timer_Err        = 0
Alloc_Mem_Err    = 0
State Mismatch   = 0
Other_Error      = 0

No-response-acct-stop packet = 0
Discarded No-response-acct-stop packet for buffer overflow = 0
```

Table 511 Description on the fields of the display radius statistics command

Field	Description
state statistic(total=1024)	State statistics

Table 511 Description on the fields of the display radius statistics command

Field	Description
DEAD	The state of idle
AuthProc	The state of waiting for authentication
AuthSucc	The state of authenticated
AcctStart	The state of accounting start
RLTSend	The state of sending real-time accounting packets
RLTWait	The state of waiting for real-time accounting
AcctStop	The state of accounting waiting stopped
OnLine	The state of online
Stop	The state of stop
Received and Sent packets statistic	Number of packets sent and received
Sent PKT total	Number of packets sent
Received PKT total	Number of packets received
RADIUS received packets statistic	Statistic of packets received by RADIUS
Code	Type of packet
Num	Total number of packets
Err	Number of error packets
Running statistic	Statistics of running packets
RADIUS received messages statistic	Number of messages received by RADIUS
Normal auth request	Number of normal authentication requests
EAP auth request	Number of EAP authentication requests
Account request	Number of accounting requests
Account off request	Number of stop-accounting requests
PKT auth timeout	Number of authentication timeout packets
PKT acct_timeout	Number of accounting timeout packets
Realtime Account timer	Number of realtime accounting requests
PKT response	Number of PKT responses
Session ctrl pkt	Number of session control packets
Normal author request	Number of normal authorization packets
Succ	Number of successful packets
RADIUS sent messages statistic	Number of messages that have been sent by RADIUS
Auth accept	Number of accepted authentication packets
Auth reject	Number of rejected authentication packets
EAP auth replying	Number of replying packets of EAP authentication
Account success	Number of accounting succeeded packets
Account failure	Number of accounting failed packets
Server ctrl req	Number of server control requests
RecError_MSG_sum	Number of received packets in error
SndMSG_Fail_sum	Number of packets that failed to be sent out
Timer_Err	Number of timer errors
Alloc_Mem_Err	Number of memory errors

Table 511 Description on the fields of the display radius statistics command

Field	Description
State Mismatch	Number of errors for mismatching status
Other_Error	Number of errors of other types
No-response-acct-stop packet	Number of times that no response was received for stop-accounting packets
Discarded No-response-acct-stop packet for buffer overflow	Number of stop-accounting packets that were buffered but then discarded due to full memory

display stop-accounting-buffer

Syntax **display stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View Any view

Parameter **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID. The ID is a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user by the user name, which is a case-sensitive string of 1 to 80 characters. The format of the *user-name* argument (for example, whether the domain name should be included) must comply with that specified for usernames to be sent to the RADIUS server in the RADIUS scheme.

Description Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, or user name.

*If receiving no response after sending a stop-accounting request to a RADIUS server, the device buffers the request and retransmits it. You can use the **retry stop-accounting** command to set the number of allowed transmission attempts.*

Related command: **reset stop-accounting-buffer**, **stop-accounting-buffer enable (HWTACACS scheme view)**, **user-name-format (HWTACACS scheme view)**, **retry stop-accounting (HWTACACS scheme view)**.

Example # Display information about the buffered stop-accounting requests from 0:0:0 to 23:59:59 on August 31, 2006.

```
<Sysname> display stop-accounting-buffer time-range 0:0:0-08/31/2002
 23:59:59-08/31/2006
Total find    0 record (0)
```

key (RADIUS scheme view)

Syntax **key** { **accounting** | **authentication** } *string*

undo key { **accounting** | **authentication** }

View RADIUS scheme view

Parameter **accounting**: Sets the shared key for RADIUS accounting packets.

authentication: Sets the shared key for RADIUS authentication/authorization packets.

string: Shared key, a case-sensitive string of up to 16 characters.

Description Use the **key** command to set the shared key for RADIUS authentication/authorization or accounting packets.

Use the **undo key** command to restore the default.

By default, no shared key is configured.

Note that:

- You must ensure that the same shared key is set on the device and the RADIUS server.
- If authentication/authorization and accounting are performed on two servers with different shared keys, you must set separate shared key for each on the device.

Related command: **display radius scheme**.

Example # Set the shared key for authentication/authorization packets to **hello** for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key authentication hello
```

Set the shared key for accounting packets to ok for RADIUS scheme radius1.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] key accounting ok
```

nas-ip (RADIUS scheme view)

Syntax **nas-ip** *ip-address*

undo nas-ip

View RADIUS scheme view

Parameter *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure. The address of a loopback interface is recommended.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related command: **radius nas-ip**.

Example # Set the IP address for the device to use as the source address of the RADIUS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] nas-ip 10.1.1.1
```

primary accounting (RADIUS scheme view)

Syntax **primary accounting** *ip-address* [*port-number*]

undo primary accounting

View RADIUS scheme view

Parameter *ip-address*: IP address of the primary accounting server.

port-number: UDP port number of the primary accounting server, which ranges from 1 to 65535.

Description Use the **primary accounting** command to configure the IP address and UDP port of the primary RADIUS accounting server.

Use the **undo primary accounting** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1813.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

Related command: **key (RADIUS scheme view)**, **radius scheme**, **state**.

Example # Set the IP address of the primary accounting server for RADIUS scheme **radius1** to 10.110.1.2 and the UDP port of the server to 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary accounting 10.110.1.2 1813
```

primary authentication (RADIUS scheme view)

Syntax **primary authentication** *ip-address* [*port-number*]

undo primary authentication

View RADIUS scheme view

Parameter *ip-address*: IP address of the primary authentication/authorization server.

port-number: UDP port number of the primary authentication/authorization server, which ranges from 1 to 65535.

Description Use the **primary authentication** command to configure the IP address and UDP port of the primary RADIUS authentication/authorization server.

Use the **undo primary authentication** command to restore the defaults.

By default, the default IP address is 0.0.0.0, and the default port number 1812.

Note that:

- After creating a RADIUS scheme, you are supposed to configure the IP address and UDP port of each RADIUS server (primary/secondary authentication/authorization or accounting server). The configuration of RADIUS servers is at your discretion except that there must be at least one authentication/authorization server and one accounting server. Besides, ensure that the RADIUS service port settings on the device are consistent with the port settings on the RADIUS servers.
- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.

Related command: **key (RADIUS scheme view)**, **radius scheme**, **state**.

Example # Set the IP address of the primary authentication/authorization server for RADIUS scheme **radius1** to 10.110.1.1 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] primary authentication 10.110.1.1 1812
```

radius client

Syntax **radius client enable**

undo radius client

View System view

Parameter None

Description Use the **radius client enable** command to enable the listening port of the RADIUS client.

Use the **undo radius client** command to disable the listening port of the RADIUS client.

By default, the listening port is enabled.

Note that when the listening port of the RADIUS client is disabled:

- The RADIUS client can either accept authentication, authorization or accounting requests or process timer messages. However, it fails to transmit and receive packets to and from the RADIUS server.
- The end account packets of online users cannot be sent out and buffered. This may cause that the RADIUS server still has the user record after a user goes offline for a period of time.
- The authentication, authorization and accounting turn to the local scheme after the RADIUS request fails if the RADIUS scheme and the local authentication, authorization and accounting scheme are configured.
- The buffered accounting packets cannot be sent out and will be deleted from the buffer when the configured maximum number of attempts is reached.

Example # Enable the listening port of the RADIUS client.

```
<Sysname> system-view
[Sysname] radius client enable
```

radius nas-ip

Syntax **radius nas-ip** *ip-address*

undo radius nas-ip

View System view

Parameter *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **radius nas-ip** command to set the IP address for the device to use as the source address of the RADIUS packets to be sent to the server.

Use the **undo radius nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the RADIUS packets to be sent to the server can avoid the situation where the packets sent back by the RADIUS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in RADIUS scheme view is only for the current RADIUS scheme, while the **radius nas-ip** command in system view is for all RADIUS schemes. However, the **nas-ip** command in RADIUS scheme view overwrites the configuration of the **radius nas-ip** command.

Related command: **nas-ip (RADIUS scheme view)**.

Example # Set the IP address for the device to use as the source address of the RADIUS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] radius nas-ip 129.10.10.1
```

radius scheme

Syntax **radius scheme** *radius-scheme-name*

undo radius scheme *radius-scheme-name*

View System view

Parameter *radius-scheme-name*: RADIUS scheme name, a case-insensitive string of 1 to 32 characters.

Description Use the **radius scheme** command to create a RADIUS scheme and enter RADIUS scheme view.

Use the **undo radius scheme** command to delete a RADIUS scheme.

By default, no RADIUS scheme is defined.

Note that:

- The RADIUS protocol is configured scheme by scheme. Every RADIUS scheme must at least specify the IP addresses and UDP ports of the RADIUS authentication/authorization/accounting servers and the parameters necessary for a RADIUS client to interact with the servers.
- A RADIUS scheme can be referenced by more than one ISP domain at the same time.
- You cannot remove the RADIUS scheme being used by online users with the **undo radius scheme** command.

Related command: **key (RADIUS scheme view)**, **retry realtime-accounting**, **timer realtime-accounting (RADIUS scheme view)**, **stop-accounting-buffer enable (HWTACACS scheme view)**, **retry stop-accounting (RADIUS scheme view)**, **server-type**, **state**, **user-name-format (RADIUS scheme view)**, **retry**, **display radius scheme**, **display radius statistics**.

Example # Create a RADIUS scheme named **radius1** and enter RADIUS scheme view.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1]
```

radius trap

Syntax **radius trap** { **accounting-server-down** | **authentication-server-down** }

undo radius trap { **accounting-server-down** | **authentication-server-down** }

View System view

Parameter **accounting-server-down**: RADIUS trap for accounting servers.

authentication-server-down: RADIUS trap for authentication servers.

Description Use the **radius trap** command to enable the RADIUS trap function.

Use the **undo radius trap** command to disable the function.

By default, the RADIUS trap function is disabled.

Note that:

- If a NAS sends an accounting or authentication request to the RADIUS server but gets no response, the NAS retransmits the request. With the RADIUS trap function enabled, when the NAS transmits the request for half of the specified maximum number of transmission attempts, it sends a trap message; when the

NAS transmits the request for the specified maximum number, it sends another trap message.

- If the specified maximum number of transmission attempts is odd, the half of the number refers to the smallest integer greater than the half of the number.

Example # Enable the RADIUS trap function for accounting servers.

```
<Sysname> system-view
[Sysname] radius trap accounting-server-down
```

reset radius statistics

Syntax **reset radius statistics**

View User view

Parameter None

Description Use the **reset radius statistics** command to clear RADIUS statistics.

Related command: **display radius scheme**.

Example # Clear RADIUS statistics.

```
<Sysname> reset radius statistics
```

reset stop-accounting-buffer

Syntax **reset stop-accounting-buffer** { **radius-scheme** *radius-scheme-name* | **session-id** *session-id* | **time-range** *start-time stop-time* | **user-name** *user-name* }

View User view

Parameter **radius-scheme** *radius-scheme-name*: Specifies a RADIUS scheme by its name, which is a string of 1 to 32 characters.

session-id *session-id*: Specifies a session by its ID, a string of 1 to 50 characters.

time-range *start-time stop-time*: Specifies a time range by its start time and end time in the format of hh:mm:ss-mm/dd/yyyy or hh:mm:ss-yyyy/mm/dd.

user-name *user-name*: Specifies a user name based on which to reset the stop-accounting buffer. The username is a case-sensitive string of 1 to 80 characters. The format of the *user-name* argument (for example, whether the domain name should be included) must comply with that specified for usernames to be sent to the RADIUS server in the RADIUS scheme.

Description Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests, which get no responses.

Related command: **stop-accounting-buffer enable (HWTACACS scheme view)**, **retry stop-accounting (HWTACACS scheme view)**, **user-name-format (HWTACACS scheme view)**, **display stop-accounting-buffer**.

Example # Clear the buffered stop-accounting requests for user **user0001@aabbcc.net**.

```
<Sysname> reset stop-accounting-buffer user-name user0001@aabbcc.net
```

Clear the buffered stop-accounting requests in the time range from 0:0:0 to 23:59:59 on August 31, 2006.

```
<Sysname> reset stop-accounting-buffer time-range 0:0:0-08/31/2002 2
3:59:59-08/31/2006
```

retry

Syntax **retry** *retry-times*

undo retry

View RADIUS scheme view

Parameter *retry-times*: Maximum number of retransmission attempts, in the range 1 to 20.

Description Use the **retry** command to set the maximum number of RADIUS retransmission attempts.

Use the **undo retry** command to restore the default.

The default value for the *retry-times* argument is 3.

Note that:

- Because RADIUS uses UDP packets to transmit data, the communication is not reliable. If the device does not receive a response to its request from the RADIUS server within the response time-out time, it will retransmit the RADIUS request. If the number of retransmission attempts exceeds the limit but the device still receives no response from the RADIUS server, the device regards that the authentication fails.
- The maximum number of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related command: **radius scheme**, **timer response-timeout (HWTACACS scheme view)**.

Example # Set the maximum number of RADIUS request transmission attempts to 5 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry 5
```

retry realtime-accounting

Syntax **retry realtime-accounting** *retry-times*

undo retry realtime-accounting

View RADIUS scheme view

Parameter *retry-times*: Maximum number of accounting request transmission attempts. It ranges from 1 to 255 and defaults to 5.

Description Use the **retry realtime-accounting** command to set the maximum number of accounting request transmission attempts.

Use the **undo retry realtime-accounting** command to restore the default.

Note that:

- A RADIUS server usually checks whether a user is online by a timeout timer. If it receives from the NAS no real-time accounting packet for a user in the timeout period, it considers that there may be line or device failure and stops accounting for the user. This may happen when some unexpected failure occurs. In this case, the NAS is required to disconnect the user in accordance. This is done by the maximum number of accounting request transmission attempts. Once the limit is reached but the NAS still receives no response, the NAS disconnects the user.
- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 3 (set with the **retry** command), and the real-time accounting interval is 12 minutes (set with the **timer realtime-accounting** command), and the maximum number of accounting request transmission attempts is 5 (set with the **retry realtime-accounting** command). In such a case, the device generates an accounting request every 12 minutes, and retransmits the request when receiving no response within 3 seconds. The accounting is deemed unsuccessful if no response is received within 3 requests. Then the device sends a request every 12 minutes, and if for 5 times it still receives no response, the device will cut the user connection.

Related command: **radius scheme**, **timer realtime-accounting (HWTACACS scheme view)**.

Example # Set the maximum number of accounting request transmission attempts to 10 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname -radius-radius1] retry realtime-accounting 10
```

retry stop-accounting (RADIUS scheme view)

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View RADIUS scheme view

Parameter *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 10 to 65,535 and defaults to 500.

Description Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

- Suppose that the RADIUS server response timeout period is 3 seconds (set with the **timer response-timeout** command), the timeout retransmission attempts is 5 (set with the **retry** command), and the maximum number of stop-accounting request transmission attempts is 20 (set with the **retry stop-accounting** command). This means that for each stop-accounting request, if the device receives no response within 3 seconds, it will initiate a new request. If still no responses are received within 5 renewed requests, the stop-accounting request is deemed unsuccessful. Then the device will temporarily store the request in the device and resend a request and repeat the whole process described above. Only when 20 consecutive attempts fail will the device discard the request.

Related command: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example # Set the maximum number of stop-accounting request transmission attempts to 1,000 for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] retry stop-accounting 1000
```

secondary accounting (RADIUS scheme view)

Syntax **secondary accounting** *ip-address* [*port-number*]

undo secondary accounting

View RADIUS scheme view

Parameter *ip-address*: IP address of the secondary accounting server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary accounting server, which ranges from 1 to 65535 and defaults to 1813.

Description Use the **secondary accounting** command to configure the IP address and UDP port of the secondary RADIUS accounting server.

Use the **undo secondary accounting** command to restore the defaults.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

Related command: **key (RADIUS scheme view)**, **radius scheme**, **state**.

Example # Set the IP address of the secondary accounting server for RADIUS scheme **radius1** to 10.110.1.1 and the UDP port of the server to 1813.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary accounting 10.110.1.1 1813
```

secondary authentication (RADIUS scheme view)

Syntax **secondary authentication** *ip-address* [*port-number*]

undo secondary authentication

View RADIUS scheme view

Parameter *ip-address*: IP address of the secondary authentication/authorization server, in dotted decimal notation. The default is 0.0.0.0.

port-number: UDP port number of the secondary authentication/authorization server, which ranges from 1 to 65535 and defaults to 1812.

Description Use the **secondary authentication** command to configure the IP address and UDP port of the secondary RADIUS authentication/authorization server.

Use the **undo secondary authentication** command to restore the defaults.

Note that:

- The IP addresses of the primary and secondary authentication/authorization servers cannot be the same. Otherwise, the configuration fails.
- The RADIUS service port configured on the device and that of the RADIUS server must be consistent.

Related command: **key (RADIUS scheme view)**, **radius scheme**, **state**.

Example # Set the IP address of the secondary authentication/authorization server for RADIUS scheme **radius1** to 10.110.1.2 and the UDP port of the server to 1812.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] secondary authentication 10.110.1.2 1812
```

security-policy-server

Syntax **security-policy-server** *ip-address*

undo security-policy-server { *ip-address* | **all** }

View RADIUS scheme view

Parameter *ip-address*: IP address of a security policy server.

all: All IP addresses

Description Use the **security-policy-server** command to configure the IP address of a security policy server.

Use the **undo security-policy-server** command to remove one or all configured IP addresses.

By default, no IP address is configured for a security policy server.

Related command: **radius nas-ip**

Example # For RADIUS scheme **radius1**, set the IP address of a security policy server to 10.110.1.2

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] security-policy-server 10.110.1.2
```

server-type

Syntax **server-type** { **extended** | **standard** }

undo server-type

View RADIUS scheme view

Parameter **extended**: Specifies the extended RADIUS server (generally CAMS), which requires the RADIUS client and RADIUS server to interact according to the procedures and packet formats provisioned by the private RADIUS protocol.

standard: Specifies the standard RADIUS server, which requires the RADIUS client end and RADIUS server to interact according to the regulation and packet format of the standard RADIUS protocol (RFC 2865/2866 or newer).

Description Use the **server-type** command to specify the RADIUS server type supported by the device.

Use the **undo server-type** command to restore the default.

By default, the supported RADIUS server type is **standard**.

Related command: **radius scheme**.

Example # Set the RADIUS server type of RADIUS scheme **radius1** to standard.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] server-type standard
```

state

Syntax **state** { **primary** | **secondary** } { **accounting** | **authentication** } { **active** | **block** }

View RADIUS scheme view

Parameter **primary**: Sets the status of the primary RADIUS server.

secondary: Sets the status of the secondary RADIUS server.

accounting: Sets the status of the RADIUS accounting server.

authentication: Sets the status of the RADIUS authentication/authorization server.

active: Sets the status of the RADIUS server to **active**, namely the normal operation state.

block: Sets the status of the RADIUS server to **block**.

Description Use the **state** command to set the status of a RADIUS server.

By default, every RADIUS server configured with an IP address in the RADIUS scheme is in the state of active.

Note that:

- When a primary server, authentication/authorization server or accounting server, fails, the device automatically turns to the secondary server.
- Once the primary server fails, the primary server transfers into the state of **block**, and the device turns to the secondary server. In this case, if the secondary server is available, the device triggers the primary server quiet timer.

After the quiet timer times out, the status of the primary server is active again and the status of the secondary server remains the same. If the secondary server fails, the device restores the status of the primary server to active immediately.

- If the primary server has resumed, the device turns to use the primary server and stops communicating with the secondary server. After accounting starts, the communication between the client and the secondary server remains unchanged.
- When both the primary server and the secondary server are in the state of blocked, you need to set the status of the secondary server to active to use the secondary server for authentication. Otherwise, the switchover will not occur.
- If one server is in the active state while the other is blocked, the switchover will not take place even if the active server is not reachable.

Related command: **radius scheme**, **primary authentication (RADIUS scheme view)**, **secondary authentication (RADIUS scheme view)**, **primary accounting (RADIUS scheme view)**, **secondary accounting (RADIUS scheme view)**.

Example # Set the status of the secondary server in RADIUS scheme **radius1** to active.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] state secondary authentication active
```

stop-accounting-buffer enable (RADIUS scheme view)

Syntax **stop-accounting-buffer enable**

undo stop-accounting-buffer enable

View RADIUS scheme view

Parameter None

Description Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the RADIUS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related command: **reset stop-accounting-buffer**, **radius scheme**, **display stop-accounting-buffer**.

Example # In RADIUS scheme **radius1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] stop-accounting-buffer enable
```

timer quiet (RADIUS scheme view)

Syntax **timer quiet** *minutes*

undo timer quiet

View RADIUS scheme view

Parameter *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related command: **display radius scheme**.

Example # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] radius scheme test1
[Sysname-radius-test1] timer quiet 10
```

timer realtime-accounting (RADIUS scheme view)

Syntax **timer realtime-accounting** *minutes*

undo timer realtime-accounting

View RADIUS scheme view

Parameter *minutes*: Real-time accounting interval in minutes, must be a multiple of 3 and in the range 3 to 60, with the default value being 12.

Description Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the RADIUS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the RADIUS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 512 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Related command: **retry realtime-accounting**, **radius scheme**.

Example # Set the real-time accounting interval to 51 minutes for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer realtime-accounting 51
```

timer response-timeout (RADIUS scheme view)

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View RADIUS scheme view

Parameter *seconds*: RADIUS server response timeout period in seconds. It ranges from 1 to 10 and defaults to 3.

Description Use the **timer response-timeout** command to set the RADIUS server response timeout timer.

Use the **undo timer** command to restore the default.

Note that:

- If a NAS receives no response from the RADIUS server in a period of time after sending a RADIUS request (authentication/authorization or accounting request), it has to resend the request so that the user has more opportunity to

obtain the RADIUS service. The NAS uses the RADIUS server response timeout timer to control the transmission interval.

- A proper value for the RADIUS server response timeout timer can help improve the system performance. Set the timer based on the network conditions.
- The maximum total number of all types of retransmission attempts multiplied by the RADIUS server response timeout period cannot be greater than 75.

Related command: **radius scheme**, **retry**.

Example # Set the RADIUS server response timeout timer to 5 seconds for RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] timer response-timeout 5
```

user-name-format (RADIUS scheme view)

Syntax **user-name-format** { **with-domain** | **without-domain** }

View RADIUS scheme view

Parameter **with-domain**: Includes the ISP domain name in the username sent to the RADIUS server.

without-domain: Excludes the ISP domain name from the username sent to the RADIUS server.

Description Use the **user-name-format** command to specify the format of the username to be sent to a RADIUS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier RADIUS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a RADIUS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a RADIUS server.
- If a RADIUS scheme defines that the username is sent without the ISP domain name, do not apply the RADIUS scheme to more than one ISP domain, thus avoiding the confused situation where the RADIUS server regards two users in different ISP domains but with the same userid as one.

Related command: **radius scheme**.

Example # Specify the device to include the domain name in the username sent to the RADIUS servers for the RADIUS scheme **radius1**.

```
<Sysname> system-view
[Sysname] radius scheme radius1
[Sysname-radius-radius1] user-name-format without-domain
```

129 HWTACACS CONFIGURATION COMMANDS

data-flow-format (HWTACACS scheme view)

Syntax **data-flow-format** { **data** { **byte** | **giga-byte** | **kilo-byte** | **mega-byte** } | **packet** { **giga-packet** | **kilo-packet** | **mega-packet** | **one-packet** } }*

undo data-flow-format { **data** | **packet** }

View HWTACACS scheme view

Parameter **data**: Specifies the unit for data flows, which can be byte, kilobyte, megabyte, or gigabyte.

packet: Specifies the unit for data packets, which can be one-packet, kilo-packet, mega-packet, or giga-packet.

Description Use the **data-flow-format** command to specify the unit for data flows or packets to be sent to a HWTACACS server.

Use the **undo data-flow-format** command to restore the default.

By default, the unit for data flows is **byte** and that for data packets is **one-packet**.

Related command: **display hwtacacs**.

Example # Define HWTACACS scheme **hwt1** to send data flows and packets destined for the HWTACACS server in kilobytes and kilo-packets.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname- hwtacacs-hwt1] data-flow-format data kilo-byte packet kilo-packet
```

display hwtacacs

Syntax **display hwtacacs** [*hwtacacs-scheme-name* [**statistics**]]

View Any view

Parameter *hwtacacs-scheme-name*: HWTACACS scheme name.

statistics: Displays complete statistics about the HWTACACS server.

Description Use the **display hwtacacs** command to display configuration information or statistics of the specified or all HWTACACS schemes.

Related command: **hwtacacs scheme**.

Example # Display configuration information about HWTACACS scheme **gy**.

```
<Sysname> display hwtacacs gy
  ------------------------------------------------------------------------
HWTACACS-server template name       : gy
  Primary-authentication-server     : 172.31.1.11:49
  Primary-authorization-server      : 172.31.1.11:49
  Primary-accounting-server         : 172.31.1.11:49
  Secondary-authentication-server   : 0.0.0.0:0
  Secondary-authorization-server    : 0.0.0.0:0
  Secondary-accounting-server       : 0.0.0.0:0
  Current-authentication-server     : 172.31.1.11:49
  Current-authorization-server      : 172.31.1.11:49
  Current-accounting-server         : 172.31.1.11:49
  NAS-IP-address                    : 0.0.0.0
  key authentication                : 790131
  key authorization                 : 790131
  key accounting                    : 790131
  Quiet-interval(min)               : 5
  Realtime-accounting-interval(min) : 12
  Response-timeout-interval(sec)    : 5
  Acct-stop-PKT retransmit times    : 100
  Domain-included                   : Yes
  Data traffic-unit                 : B
  Packet traffic-unit               : one-packet
  ------------------------------------------------------------------------
```

Table 513 Description on the fields of the display hwtacacs command

Field	Description
HWTACACS-server template name	Name of the HWTACACS scheme
Primary-authentication-server	Primary authentication server
Primary-authorization-server	Primary authorization server
Primary-accounting-server	Primary accounting server
Secondary-authentication-server	Secondary authentication server
Secondary-authorization-server	Secondary authorization server
Secondary-accounting-server	Secondary accounting server
Current-authentication-server	Currently used authentication server
Current-authorization-server	Currently used authorization server
Current-accounting-server	Currently used accounting server
NAS-IP-address	NAS-IP address
key authentication	Key for authentication
key authorization	Key for authorization
key accounting	Key for accounting
Quiet-interval	Quiet interval for the primary server
Realtime-accounting-interval	Real-time accounting interval

Table 513 Description on the fields of the display hwtacacs command

Field	Description
Response-timeout-interval	Server response timeout period
Acct-stop-PKT retransmit times	Number of stop-accounting packet transmission retries
Domain-included	Whether a user name includes the domain name
Data traffic-unit	Unit for data flows
Packet traffic-unit	Unit for data packets

display stop-accounting-buffer

Syntax **display stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*

View Any view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

Description Use the **display stop-accounting-buffer** command to display information about the stop-accounting requests buffered in the device by scheme, session ID, time range, user name, or slot.

Related command: **reset stop-accounting-buffer**, **stop-accounting-buffer enable (HWTACACS scheme view)**, **retry stop-accounting (HWTACACS scheme view)**.

Example # Display information about the buffered stop-accounting requests for HWTACACS scheme **hwt1**.

```
<Sysname> display stop-accounting-buffer hwtacacs-scheme hwt1
Total 0 record(s) Matched
```

hwtacacs nas-ip

Syntax **hwtacacs nas-ip** *ip-address*

undo hwtacacs nas-ip

View System view

Parameter *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **hwtacacs nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo hwtacacs nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related command: **nas-ip (HWTACACS scheme view)**.

Example # Set the IP address for the device to use as the source address of the HWTACACS packets to 129.10.10.1.

```
<Sysname> system-view
[Sysname] hwtacacs nas-ip 129.10.10.1
```

hwtacacs scheme

Syntax **hwtacacs scheme** *hwtacacs-scheme-name*

undo hwtacacs scheme *hwtacacs-scheme-name*

View System view

Parameter *hwtacacs-scheme-name*: HWTACACS scheme name, a case-insensitive string of 1 to 32 characters.

Description Use the **hwtacacs scheme** command to create an HWTACACS scheme and enter HWTACACS scheme view.

Use the **undo hwtacacs scheme** command to delete an HWTACACS scheme.

By default, no HWTACACS scheme exists.

Example # Create an HWTACACS scheme named **hwt1** and enter HWTACACS scheme view.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1]
```

key (HWTACACS scheme view)

Syntax **key** { **accounting** | **authentication** | **authorization** } *string*

undo key { **accounting** | **authentication** | **authorization** } *string*

View HWTACACS scheme view

Parameter **accounting**: Sets the shared key for HWTACACS accounting packets.

authentication: Sets the shared key for HWTACACS authentication packets.

authorization: Sets the shared key for HWTACACS authorization packets.

string: Shared key, a string of 1 to 16 characters.

Description Use the **key** command to set the shared key for HWTACACS authentication, authorization, or accounting packets.

Use the **undo key** command to remove the configuration.

By default, no shared key is configured.

Related command: **display hwtacacs**.

Example # Set the shared key for HWTACACS accounting packets to **hello** for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] key accounting hello
```

nas-ip (HWTACACS scheme view)

Syntax **nas-ip** *ip-address*

undo nas-ip

View HWTACACS scheme view

Parameter *ip-address*: IP address in dotted decimal notation. It must be an address of the device and cannot be all 0s address, all 1s address, a class D address, a class E address or a loopback address.

Description Use the **nas-ip** command to set the IP address for the device to use as the source address of the HWTACACS packets to be sent to the server.

Use the **undo nas-ip** command to remove the configuration.

By default, the source IP address of a packet sent to the server is the IP address of the outbound port.

Note that:

- Specifying a source address for the HWTACACS packets to be sent to the server can avoid the situation where the packets sent back by the HWTACACS server cannot reach the device as the result of a physical interface failure.
- If you configure the command for more than one time, the last configuration takes effect.
- The **nas-ip** command in HWTACACS scheme view is only for the current HWTACACS scheme, while the **hwtacacs nas-ip** command in system view is for all HWTACACS schemes. However, the **nas-ip** command in HWTACACS scheme view overwrites the configuration of the **hwtacacs nas-ip** command.

Related command: **hwtacacs nas-ip**.

Example # Set the IP address for the device to use as the source address of the HWTACACS packets to 10.1.1.1.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] nas-ip 10.1.1.1
```

primary accounting (HWTACACS scheme view)

Syntax **primary accounting** *ip-address* [*port-number*]

undo primary accounting

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary accounting** command to specify the primary HWTACACS accounting server.

Use the **undo primary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.

- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Example # Configure the primary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme test1
[Sysname-hwtacacs-test1] primary accounting 10.163.155.12 49
```

primary authentication (HWTACACS scheme view)

Syntax **primary authentication** *ip-address* [*port-number*]

undo primary authentication

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary authentication** command to specify the primary HWTACACS authentication server.

Use the **undo primary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related command: **display hwtacacs**.

Example # Set the primary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authentication 10.163.155.13 49
```

primary authorization

Syntax **primary authorization** *ip-address* [*port-number*]

undo primary authorization

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **primary authorization** command to specify the primary HWTACACS authorization server.

Use the **undo primary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related command: **display hwtacacs**.

Example # Configure the primary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] primary authorization 10.163.155.13 49
```

reset hwtacacs statistics

Syntax **reset hwtacacs statistics** { **accounting** | **all** | **authentication** | **authorization** }

View User view

Parameter **accounting**: Clears HWTACACS accounting statistics.

all: Clears all HWTACACS statistics.

authentication: Clears HWTACACS authentication statistics.

authorization: Clears HWTACACS authorization statistics.

Description Use the **reset hwtacacs statistics** command to clear HWTACACS statistics.

Related command: **display hwtacacs**.

Example # Clear all HWTACACS statistics.

```
<Sysname> reset hwtacacs statistics all
```

reset stop-accounting-buffer

Syntax **reset stop-accounting-buffer hwtacacs-scheme** *hwtacacs-scheme-name*

View User view

Parameter **hwtacacs-scheme** *hwtacacs-scheme-name*: Specifies a HWTACACS scheme by its name, a string of 1 to 32 characters.

Description Use the **reset stop-accounting-buffer** command to clear the buffered stop-accounting requests that get no responses.

Related command: **stop-accounting-buffer enable (HWTACACS scheme view)**, **retry stop-accounting (HWTACACS scheme view)**, **display stop-accounting-buffer**.

Example # Clear the buffered stop-accounting requests for HWTACACS scheme **hwt1**.

```
<Sysname> reset stop-accounting-buffer hwtacacs-scheme hwt1
```

retry stop-accounting (HWTACACS scheme view)

Syntax **retry stop-accounting** *retry-times*

undo retry stop-accounting

View HWTACACS scheme view

Parameter *retry-times*: Maximum number of stop-accounting request transmission attempts. It ranges from 1 to 300 and defaults to 100.

Description Use the **retry stop-accounting** command to set the maximum number of stop-accounting request transmission attempts.

Use the **undo retry stop-accounting** command to restore the default.

Related command: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Example # Set the maximum number of stop-accounting request transmission attempts to 50.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] retry stop-accounting 50
```

secondary accounting (HWTACACS scheme view)

Syntax **secondary accounting** *ip-address* [*port-number*]

undo secondary accounting

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary accounting** command to specify the secondary HWTACACS accounting server.

Use the **undo secondary accounting** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary accounting servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an accounting server only when no active TCP connection for sending accounting packets is using it.

Example # Configure the secondary accounting server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary accounting 10.163.155.12 49
```

secondary authentication (HWTACACS scheme view)

Syntax **secondary authentication** *ip-address* [*port-number*]

undo secondary authentication

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary authentication** command to specify the secondary HWTACACS authentication server.

Use the **undo secondary authentication** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authentication servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authentication server only when no active TCP connection for sending authentication packets is using it.

Related command: **display hwtacacs**.

Example # Configure the secondary authentication server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authentication 10.163.155.13 49
```

secondary authorization

Syntax **secondary authorization** *ip-address* [*por-number t*]

undo secondary authorization

View HWTACACS scheme view

Parameter *ip-address*: IP address of the server, a valid unicast address in dotted decimal notation. The default is 0.0.0.0.

port-number: Port number of the server. It ranges from 1 to 65535 and defaults to 49.

Description Use the **secondary authorization** command to specify the secondary HWTACACS authorization server.

Use the **undo secondary authorization** command to remove the configuration.

Note that:

- The IP addresses of the primary and secondary authorization servers cannot be the same. Otherwise, the configuration fails.
- The HWTACACS service port configured on the device and that of the HWTACACS server must be consistent.
- If you configure the command for more than one time, the last configuration takes effect.
- You can remove an authorization server only when no active TCP connection for sending authorization packets is using it.

Related command: **display hwtacacs**.

Example # Configure the secondary authorization server.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] secondary authorization 10.163.155.13 49
```

stop-accounting-buffer enable (HWTACACS scheme view)

Syntax **stop-accounting-buffer enable**

undo stop-accounting-buffer enable

View HWTACACS scheme view

Parameter None

Description Use the **stop-accounting-buffer enable** command to enable the device to buffer stop-accounting requests getting no responses.

Use the **undo stop-accounting-buffer enable** command to disable the device from buffering stop-accounting requests getting no responses.

By default, the device is enabled to buffer stop-accounting requests getting no responses.

Since stop-accounting requests affect the charge to users, a NAS must make its best effort to send every stop-accounting request to the HWTACACS accounting servers. For each stop-accounting request getting no response in the specified period of time, the NAS buffers and resends the packet until it receives a response or the number of transmission retries reaches the configured limit. In the latter case, the NAS discards the packet.

Related command: **reset stop-accounting-buffer**, **hwtacacs scheme**, **display stop-accounting-buffer**.

Example # In HWTACACS scheme **hwt1**, enable the device to buffer the stop-accounting requests getting no responses.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] stop-accounting-buffer enable
```

timer quiet (HWTACACS scheme view)

Syntax **timer quiet** *minutes*

undo timer quiet

View HWTACACS scheme view

Parameter *minutes*: Primary server quiet period, in minutes. It ranges from 1 to 255 and defaults to 5.

Description Use the **timer quiet** command to set the quiet timer for the primary server, that is, the duration that the status of the primary server stays blocked before resuming the active state.

Use the **undo timer quiet** command to restore the default.

Related command: **display hwtacacs**.

Example # Set the quiet timer for the primary server to 10 minutes.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer quiet  10
```

timer realtime-accounting (HWTACACS scheme view)

Syntax **timer realtime-accounting** *minutes*

undo timer realtime-accounting

View HWTACACS scheme view

Parameter *minutes*: Real-time accounting interval in minutes. It is a multiple of 3 in the range 3 to 60 and defaults to 12.

Description Use the **timer realtime-accounting** command to set the real-time accounting interval.

Use the **undo timer realtime-accounting** command to restore the default.

Note that:

- For real-time accounting, a NAS must transmit the accounting information of online users to the HWTACACS accounting server periodically. This command is for setting the interval.
- The setting of the real-time accounting interval somewhat depends on the performance of the NAS and the HWTACACS server: a shorter interval requires higher performance. You are therefore recommended to adopt a longer interval when there are a large number of users (more than 1000, inclusive). The following table lists the recommended ratios of the interval to the number of users.

Table 514 Recommended ratios of the accounting interval to the number of users

Number of users	Real-time accounting interval (minute)
1 to 99	3
100 to 499	6
500 to 999	12
1000 or more	15 or more

Example # Set the real-time accounting interval to 51 minutes for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer realtime-accounting 51
```

timer response-timeout (HWTACACS scheme view)

Syntax **timer response-timeout** *seconds*

undo timer response-timeout

View HWTACACS scheme view

Parameter *seconds*: HWTACACS server response timeout period in seconds. It ranges from 1 to 300 and defaults to 5.

Description Use the **timer response-timeout** command to set the HWTACACS server response timeout timer.

Use the **undo timer** command to restore the default.

As HWTACACS is based on TCP, the timeout of the server response timeout timer and/or the TCP timeout timer will cause the device to be disconnected from the HWTACACS server.

Related command: **display hwtacacs**.

Example # Set the HWTACACS server response timeout timer to 30 seconds for HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] timer response-timeout 30
```

user-name-format (HWTACACS scheme view)

Syntax **user-name-format** { **with-domain** | **without-domain** }

View HWTACACS scheme view

Parameter **with-domain**: Includes the ISP domain name in the username sent to the HWTACACS server.

without-domain: Excludes the ISP domain name from the username sent to the HWTACACS server.

Description Use the **user-name-format** command to specify the format of the username to be sent to a HWTACACS server.

By default, the ISP domain name is included in the username.

Note that:

- A username is generally in the format of userid@isp-name, of which isp-name is used by the device to determine the ISP domain to which a user belongs. Some earlier HWTACACS servers, however, cannot recognize a username including an ISP domain name. Before sending a username including a domain name to such a HWTACACS server, the device must remove the domain name. This command is thus provided for you to decide whether to include a domain name in a username to be sent to a HWTACACS server.
- If a HWTACACS scheme defines that the username is sent without the ISP domain name, do not apply the HWTACACS scheme to more than one ISP domain, thus avoiding the confused situation where the HWTACACS server regards two users in different ISP domains but with the same userid as one.

Related command: **hwtacacs scheme**.

Example # Specify the device not to include the ISP domain name in the username sent to the HWTACACS servers for the HWTACACS scheme **hwt1**.

```
<Sysname> system-view
[Sysname] hwtacacs scheme hwt1
[Sysname-hwtacacs-hwt1] user-name-format without-domain
```

130 PACKET FILTER FIREWALL CONFIGURATION COMMANDS

The term "router" in this document refers to a router in a generic sense or a Layer 3 switch running a routing protocol.

display firewall ethernet-frame-filter

Syntax **display firewall ethernet-frame-filter** { **all** | **dlsw** | **interface** *interface-type interface number* }

View Any view

Parameter **all**: Displays all the firewall statistics information.

dlsw: Displays the firewall statistics information of packets passing the DLSw module. *interface-type interface-number*: Specifies an interface by it type and number.

Description Use the **display firewall ethernet-frame-filter** command to view the Ethernet frame filtering statistics.

Example # Display the Ethernet frame filtering statistics on Ethernet 1/0.

```
<Sysname> display firewall ethernet-frame-filter interface ethernet 1/0
Interface: Ethernet1/0
  In-bound Policy: acl 4000
        From 2005-06-07 14:46:59  to 2005-06-07 16:16:23
            0 packets, 0 bytes, 0% permitted,
            0 packets, 0 bytes, 0% denied,
            0 packets, 0 bytes, 0% permitted default,
            0 packets, 0 bytes, 0% denied default,
       Totally 0 packets, 0 bytes, 0% permitted,
       Totally 0 packets, 0 bytes, 0% denied.
  Out-bound Policy: acl 4000
       From 2005-06-07 15:59:23  to 2005-06-07 16:16:23
            0 packets, 0 bytes, 0% permitted,
            0 packets, 0 bytes, 0% denied,
            0 packets, 0 bytes, 0% permitted default,
            0 packets, 0 bytes, 0% denied default,
       Totally 0 packets, 0 bytes, 0% permitted,
       Totally 0 packets, 0 bytes, 0% denied.
```

Table 515 Description on the fields of display firewall ethernet-frame-filter

Field	Description
Interface	Name of the ACL configured interface
In-bound Policy	Indicates an inbound ACL rule has been configured on the interface

Table 515 Description on the fields of display firewall ethernet-frame-filter

Field	Description
Out-bound Policy	Indicates an outbound ACL rule has been configured on the interface.

display firewall-statistics

Syntax **display firewall-statistics** { **all** | **interface** *interface-type interface-num* | **fragments-inspect** }

View Any view

Parameter **all**: Displays the firewall statistics on all interfaces.

interface-type interface-num: Displays the firewall statistics about the specified interface.

fragments-inspect: Displays statistics about fragments inspection.

Description Use the **display firewall-statistics** command to view the statistics of the firewall.

Related command: **firewall fragments-inspect**.

At most 50 fragments with the same 16-bit identifier in IP header can be recorded.

Example # Display statistics information about fragments inspection.

```
<Sysname> display firewall-statistics fragments-inspect
  Fragments inspection is enabled.
  The high-watermark for clamping is 10000.
  The low-watermark for clamping is 1000.
  Current records for fragments inspection is 0.
```

Table 516 Description on the fields of the display firewall-statistics command

Field	Description
Fragments inspection is enabled	The fragments inspection function of the firewall is enabled
The high-watermark for clamping	The high watermark value of the number of fragment status records
The low-watermark for clamping	The low watermark value of the number of fragment status records
Current records for fragments inspection	The current number of records for fragments inspection

firewall default

Syntax **firewall default** { **permit** | **deny** }

View System view

Parameter **permit**: Sets the default filtering action to "permit".

deny: Sets the default filtering action to "deny".

Description Use the **firewall default** command to set the default filtering action of the firewall to "permit" or "deny".

By default, the default filtering action is "permit", which applies to traffic not defined by the ACLs.

Example # Set the default filtering mode of the firewall to "deny".

```
<Sysname> system-view
[Sysname] firewall enable
```

firewall enable

Syntax **firewall enable**

undo firewall enable

View System view

Parameter None

Description Use the **firewall enable** command to enable the firewall.

Use the **undo firewall enable** command to disable the firewall.

By default, the firewall is disabled.

Example # Enable the firewall.

```
<Sysname> system-view
[Sysname] firewall enable
```

firewall ethernet-frame-filter

Syntax **firewall ethernet-frame-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** }

undo firewall ethernet-frame-filter { **inbound** | **outbound** }

View Interface view

Parameter *acl-number*: Layer 2 ACL number, in the range 4000 to 4999.

name *acl-name*: Specifies the Layer 2 ACL name, a case-insensitive string of 1 to 32 characters that must start with an English letter a to z or A to Z. To avoid confusion, the word "all" cannot be used as the ACL name.

inbound: Filters packets in the inbound direction.

outbound: Filters packets in the outbound direction.

Description Use the **firewall ethernet-frame-filter** command to configure Ethernet frame filtering.

Use the **undo firewall ethernet-frame-filter** command to remove the Ethernet frame filtering.

Ethernet frame filtering is not performed by default.

Example # Configure Ethernet frame filtering rules on the inbound direction of interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] bridge enable
[Sysname] bridge 1 enable
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] bridge-set 1
[Sysname-Etherhet1/0] firewall ethernet-frame-filter 4001 inbound
```

firewall fragments-inspect

Syntax **firewall fragments-inspect**

undo firewall fragments-inspect

View System view

Parameter None

Description Use the **firewall fragments-inspect** command to enable fragments inspection.

Use the **undo firewall fragments-inspect** command to disable fragments inspection.

Be default, fragments inspection is disabled.

Related command: **firewall fragments-inspect**, and **firewall packet-filter**.

Example # Enable fragments inspection.

```
<Sysname> system-view
[Sysname] firewall fragments-inspect
```

firewall fragments-inspect [high | low]

Syntax **firewall fragments-inspect** [**high** | **low**] { *number* | **default** }

undo firewall fragments-inspect [**high** | **low**]

View System view

Parameter **high** *number*: Specifies the high watermark value of the number of fragment status records.

low *number*: Specifies the low watermark value of the number of fragment status records.

default: Specifies the default number of fragment status records.

Description Use the **firewall fragments-inspect** [**high** | **low**] command to configure the high and low watermark values for fragments inspection.

Use the **undo firewall fragments-inspect** [**high** | **low**] command to restore the default high and low watermark values.

By default, the high watermark value is 2,000 and low watermark value is 1500.

The low watermark value must be smaller than or equal to the high watermark value.

Related command: **firewall fragments-inspect** and **firewall packet-filter**.

Example # Set the high watermark for fragment inspection to 3,000 and low watermark to the default value.

```
<Sysname> system-view
[Sysname] firewall fragments-inspect high 3000
[Sysname] firewall fragments-inspect low default
```

firewall ipv6 fragments-inspect

Syntax **firewall ipv6 fragments-inspect**

undo firewall ipv6 fragments-inspect

View System view

Parameter None

Description Use the **firewall ipv6 fragments-inspect** command to enable IPv6 fragments inspection.

Use the **undo firewall ipv6 fragments-inspect** command to disable IPv6 fragments inspection.

By default, IPv6 fragments inspection is disabled.

Example # Enable IPv6 fragments inspection.

```
<Sysname> system-view
[Sysname] firewall ipv6 fragments-inspect
```

firewall packet-filter

Syntax **firewall packet-filter** { *acl-number* | **name** *acl-name* } { **inbound** | **outbound** } [**match-fragments** { **normally** | **exactly** }]

undo firewall packet-filter *acl-number* { **inbound** | **outbound** }

View Interface view

Parameter *acl-number*: Basic ACL number, in the range 2000 to 2999; advanced ACL number, in the range 3000 to 3999.

name *acl-name*: Specifies the name of a basic or advanced IPv4 ACL, a case-insensitive string of 1 to 32 characters that must start with an English letter a to z or A to Z. To avoid confusion, the word "all" cannot be used as the ACL name.

inbound: Filters packets in the inbound direction.

outbound: Filters packets in the outbound direction.

match-fragments: Specifies the fragment match mode (for advanced ACLs only).

normally: Specifies the normal match mode, which is the default mode.

exactly: Specifies the exact match mode.

Description Use the **firewall packet-filter** command to configure IPv4 packet filtering on the interface.

Use the **undo firewall packet-filter** command to cancel the configuration.

Packets are not filtered on an interface by default.

Related command: **firewall fragments-inspect**.

Example # Apply ACL 2001 on Serial 2/0 to filter packets forwarded by the interface.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] firewall packet-filter 2001 outbound
```

firewall packet-filter ipv6

Syntax **firewall packet-filter ipv6** { *acl6-number* | **name** *acl6-name* } { **inbound** | **outbound** }

undo firewall packet-filter ipv6 { **inbound** | **outbound** }

View Interface view

Parameter *acl-number*: Basic ACL number, in the range 2000 to 2999; advanced ACL number, in the range 3000 to 3999.

name *acl6-name*: Specifies the name of a basic or advanced IPv6 ACL, a case-insensitive string of 1 to 32 characters that must start with an English letter a to z or A to Z. To avoid confusion, the word "all" cannot be used as the ACL name.

inbound: Filters packets in the inbound direction.

outbound: Filters packets in the outbound direction.

Description Use the **firewall packet-filter ipv6** command to configure IPv6 packet filtering on the interface.

Use the **undo firewall packet-filter ipv6** command to remove the IPv6 packet filtering setting on the interface.

By default, IPv6 packets are not filtered on the interface.

Example # Configure IPv6 packet filtering for Ethernet 1/0 using IPv6 ACL 2500.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] firewall packet-filter ipv6 2500 outbound
```

reset firewall ethernet-frame-filter

Syntax **reset firewall ethernet-frame-filter** { **all** | **dlsw** | **interface** *interface-type interface number* }

View User view

Parameter **all**: Removes all firewall statistics.

dlsw: Removes the firewall statistics of the DLSw module.

interface-type interface-number: Specifies an interface by its type and number.

Description Use the **reset firewall ethernet-frame-filter** command to clear the Ethernet frame filtering statistics.

Example # Clear all the firewall statistic information.

```
<Sysname> reset firewall ethernet-frame-filter all
```

reset firewall-statistics

Syntax **reset firewall-statistics** { **all** | **interface** *interface-type interface-num* }

View User view

Parameter **all**: Clears the firewall statistic information on all interfaces.

interface *interface-type interface-num*: Clears the firewall statistic information of the specified interface.

Description Use the **reset firewall-statistics** command to clear the statistic information of the firewall.

Example # Clear the firewall statistic information of Ethernet 1/0.

```
<Sysname> reset firewall-statistics interface ethernet 1/0
```

131
ASPF CONFIGURATION COMMANDS

aging-time

Syntax **aging-time** { **syn** | **fin** | **tcp** | **udp** } *seconds*

undo aging-time { **syn** | **fin** | **tcp** | **udp** }

View ASPF policy view

Parameter **syn**: Specifies that the TCP session will be terminated *seconds* seconds after a SYN is detected if the session fails to reach the established state.

fin: Specifies that the TCP session will be terminated *seconds* seconds after a FIN is detected.

tcp: Specifies, together with the *seconds* argument, the idle timeout of a TCP session.

udp: Specifies, together with the *seconds* argument, the idle timeout of a UDP "session".

seconds: Idle timeout period of the session, in seconds. The effective range is 5 to 43,200.

Description Use the **aging-time** command to configure the SYN/FIN wait timeout period of a TCP session or the idle timeout period of a TCP session/UDP "session".

Use the **undo aging-time** command to restore the inactivity timeout period to the default value.

By default, the SYN, FIN, TCP and UDP timeout period values are 30, 5, 3,600 and 30 seconds respectively.

Within the timeout period, the system maintains the established session.

Related command: **display aspf all**, **display aspf policy**, **display aspf session**, and **display aspf interface**.

Example # Create an ASPF policy, the number of which is 1.

```
<Sysname> system-view
[Sysname] aspf-policy 1
```

Set the SYN wait timeout period of the TCP session to 20 seconds.

```
[Sysname-aspf-policy-1] aging-time syn 20
```

Set the FIN wait timeout period of the TCP session to 10 seconds.

```
[Sysname-aspf-policy-1] aging-time fin 10
```

Set the TCP idle timeout period to 3000 seconds.

```
[Sysname-aspf-policy-1] aging-time tcp 3000
```

Set the UDP idle timeout period to 110 seconds.

```
[Sysname-aspf-policy-1] aging-time udp 110
```

aspf-policy

Syntax **aspf-policy** *aspf-policy-number*

undo aspf-policy *aspf-policy-number*

View System view

Parameter *aspf-policy-number*: ASPF policy number, in the range of 1 to 99

Description Use the **aspf-policy** command to create an ASPF policy and enter its view.

Use the **undo aspf-policy** command to remove an ASPF policy.

A defined ASPF policy can be applied through its policy number.

Example # Create an ASPF policy and enter the corresponding ASPF policy view.

```
<Sysname> system-view
[Sysname] aspf-policy 1
[Sysname-aspf-policy-1]
```

detect

Syntax **detect** *protocol* [**java-blocking** *acl-number*] [**aging-time** *seconds*]

undo detect *protocol*

View ASPF policy view

Parameter *protocol*: Name of a protocol supported by the ASPF. Application layer protocols include FTP, HTTP, H.323, SMTP, and RTSP, and transport layer protocols include TCP and UDP.

java-blocking: Blocks the Java Applets of packets to the specified network segment, applicable to HTTP only.

acl-number: Basic ACL number, in the range 2,000 to 2,999.

seconds: Configures the protocol idle timeout period, in seconds. The effective range is 5 to 43,200.

Description Use the **detect** command to configure ASPF detection for the application layer protocol or transport layer protocol.

Use the **undo detect** command to remove the configuration.

By default, the timeout period for an application layer protocol is 3,600 seconds, the TCP-based timeout period is 3,600 seconds, and the UDP-based timeout period is 30 seconds.

Note that:

- If the protocol type is HTTP, Java blocking is allowed.
- If application layer protocol detection and general TCP/UDP detection are both enables, application layer protocol detection is given priority over general TCP/UDP detection.
- ASPF uses timeouts to manage the session status information of a protocol so as to determine when to terminate the status information management of a session or when to delete a session that cannot be normally established. As a global configuration, the setting of a timeout applies to all sessions to protect system resources from being maliciously seized.
- A protocol idle timeout setting specified using the **detect** command has priority over a timeout setting specified using the **aging-time** command.

Related command: **display aspf all**, **display aspf policy**, **display aspf session**, and **display aspf interface**.

Example # Specify ASPF policy 1 for the FTTP protocol, enable Java blocking, and configure ACL 2000 so that the ASPF policy can filter Java applets from the server 10.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 10.1.1.1 0
[Sysname-acl-basic-2000] rule deny source any
[Sysname-acl-basic-2000] quit
[Sysname] aspf-policy 1
[Sysname-aspf-policy-1] detect http java-blocking 2000
```

display aspf all

Syntax **display aspf all**

View Any view

Parameter None

Description Use the **display aspf all** command to view the information of all the ASPF policies and sessions.

Example # Display the information of all the ASPF policies and sessions.

```
<Sysname> display aspf all
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                disable
    SYN timeout:        30    s
    FIN timeout:        5     s
    TCP timeout:        3600  s
    UDP timeout:        30    s
    Detect Protocols:
      ftp  timeout 3600 s
      tcp  timeout 3600 s

[Interface Configuration]
   Interface                    InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   Ethernet1/1                 none            1
[Established Sessions]
Session Initiator           Responder           Application    Status
------------------------------------------------------------------------------
73A4844 1.1.1.50:1025         2.2.2.1:21            ftp             FTP_CONXN_UP
```

Table 517 Description of the fields of the display aspf all command

Field	Description
SYN timeout	SYN timeout value of the TCP session
FIN timeout	FIN timeout of the TCP session
TCP timeout	Idle timeout of the TCP session.
UDP timeout	Idle timeout of the UDP session.
Detect Protocols	Detect protocols
InboundPolicy	Inbound ASPF policy
OutboundPolicy	Outbound ASPF policy
Detect Protocols	Detected protocols
Session	Session ID
Initiator	IP address and port number of the Initiator of the session
Responder	IP address and port number of the responder of the session
Application	Application protocol
Status	Session status

display aspf interface

Syntax **display aspf interface**

View Any view

Parameter None

Description Use the **display aspf interface** command to view the ASPF policy configuration applied on interfaces.

Example # Display the ASPF information on the interface(s).

```
<Sysname> display aspf interface
[Interface Configuration]
   Interface                      InboundPolicy   OutboundPolicy
 ----------------------------------------------------------------
   Serial2/1                    1               none
```

Table 518 Description of the fields of the display aspf interface command

Field	Description
InboundPolicy	Inbound ASPF policy
OutboundPolicy	Outbound ASPF policy

display aspf policy

Syntax **display aspf policy** *aspf-policy-number*

View Any view

Parameter *aspf-policy-number*: ASPF policy number, in the range 1 to 99

Description Use the **display aspf policy** command to view the information of an ASPF policy.

Example # Display the configuration information of ASPF policy 1.

```
<Sysname> display aspf policy 1
[ASPF Policy Configuration]
  Policy Number 1:
    Log:                 disable
    SYN timeout:         30    s
    FIN timeout:         5     s
    TCP timeout:         3600  s
    UDP timeout:         30    s
    Detect Protocols:
      ftp  timeout 120 s
      tcp  timeout 3600 s
```

display aspf session

Syntax **display aspf session** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed information of the current session.

Description Use the **display aspf session** command to view the information of the current ASPF session.

Example # Display the related information of the current ASPF session.

```
<Sysname> display aspf session
[Established Sessions]
Session Initiator           Responder        Application   Status
212BA84 169.254.1.121:1427  169.254.1.52:0   ftp-data      TCP_DOWN
7148124 100.1.1.1:1027      200.1.1.2:21     ftp           FTP_CONXN_UP
```

Display the detailed information of the current ASPF session.

```
<Sysname> display aspf session verbose
[Session 0x7148124]
   Initiator: 100.1.1.1:1027         Responder: 200.1.1.2:21
   Application protocol: ftp         Status: FTP_CONXN_UP
   Transport protocol: 6             Port: 21
   Child: 0x0                        Parent: 0x0
   Interface: Ethernet1/1            Direction: outbound
   Timeout 01:00:00                  Time left 01:00:00
   Initiator Bytes/Packets sent: 350/8
   Responder Bytes/Packets sent: 324/6
   Initiator tcp SeqNumber/AckNumber: 141385146/134665684
   Responder tcp SeqNumber/AckNumber: 134665683/141385146
```

Table 519 Description of the fields of the display aspf session command

Field	Description
Initiator	IP address and port number of the initiator of the session
Responder	IP address and port number of the responder of the session
Application protocol	Application protocol
Status	Status of the session
Transport protocol	Protocol number of the transport layer
Port	Port number of the application layer protocol
Child	Child session
Parent	Parent session
Interface: Ethernet1/1 Direction: outbound	The ASPF policy is applied on the inbound direction of Ethernet 1/1
Timeout	Timeout set for the protocol
Time left	Remaining timeout period
Initiator Bytes/Packets sent	Number of initiator bytes/packets sent
Responder Bytes/Packets sent	Number of responder bytes/packets sent
Initiator tcp SeqNumber/AckNumber	TCP sequence number/acknowledgment number of the initiator
Responder tcp SeqNumber/AckNumber	TCP sequence number/acknowledgment number of the responder

display port-mapping

Syntax **display port-mapping** [*application-name* | **port** *port-number*]

View Any view

Parameter *application-name*: Name of the application to be used for port mapping Available applications include FTP, HTTP, H.323, SMTP, and RTSP.

port-number: Port number, in the range 0 to 65535

Description Use the **display port-mapping** command to view port mapping information.

Related command: **port-mapping**.

Example # Display all the information about port mapping.

```
<Sysname> display port-mapping
  SERVICE    PORT       ACL        TYPE
 ------------------------------------------------
  ftp          21                  system defined
  smtp         25                  system defined
  http         80                  system defined
  rtsp        554                  system defined
  H.323       1720                  system defined
  http       8080                  user   defined
```

firewall aspf

Syntax **firewall aspf** *aspf-policy-number* { **inbound** | **outbound** }

undo firewall aspf *aspf-policy-number* { **inbound** | **outbound** }

View Interface view

Parameter *aspf-policy-number*: Number of the ASPF policy, in the range 1 to 99.

inbound: Applies ASPF policy to inbound packets.

outbound: Applies ASPF policy to outbound packets.

Description Use the **firewall aspf** command to apply the specified ASPF policy on the specified direction of the current interface.

Use the **undo firewall aspf** command to remove the specified ASPF policy applied on the specified direction of the current interface.

By default, ASPF policy is not applied on the interface.

Example # Apply the configured ASPF firewall policy on the outbound direction of Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] firewall aspf 1 outbound
```

log enable

Syntax **log enable**

undo log enable

View ASPF policy view

Parameter None

Description Use the **log enable** command to enable the session logging function of an ASPF.

Use the **undo log enable** command to disable the session logging function.

By default, the session logging function is disabled.

The enhanced session logging function of an ASPF can record the information of each connection, including the duration, source address and destination address of the connection, the port used by the connection and number of bytes transmitted.

Related command: **display aspf all**, **display aspf policy**, **display aspf session**, and **display aspf interface**.

Example # Enable the session logging function of the ASPF.

```
<Sysname> system-view
[Sysname] aspf-policy 1
[Sysname-aspf-policy-1] log enable
```

port-mapping

Syntax **port-mapping** *application-name* **port** *port-number* [**acl** *acl-number*]

undo port-mapping [*application-name* **port** *port-number* [**acl** *acl-number*]]

View System view

Parameter *application-name*: Name of the application for port mapping Available applications include FTP, HTTP, H.323, SMTP, and RTSP.

port-number: Port number, in the range 0 to 65535

acl-number: Basic ACL number, in the range 2000 to 2999, used to specify the host range.

Description Use the **port-mapping** command to map a port to an application layer protocol.

Use the **undo port-mapping** command to remove a port mapping entry.

By default, there is no mapping between the port and the application layer.

Related command: **display port-mapping**.

Example # Map port 3456 to the FTP protocol.

```
<Sysname> system-view
[Sysname] port-mapping ftp port 3456
```

reset aspf session

Syntax **reset aspf session**

View User view

Parameter None

Description Use the **reset aspf session** command clear ASPF sessions

Example # Clear ASPF sessions.

```
<Sysname> reset aspf session
```

132 MAC AUTHENTICATION CONFIGURATION COMMANDS

MAC authentication is not supported on the fixed layer 2 interface of FIC-4FSW, DFIC-9FSW and MSR 20 Series Products.

display mac-authentication

Syntax **display mac-authentication** [**interface** *interface-list*]

View Any view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port. With an interface range, the end interface number and the start interface number must be of the same type and the former must be greater than the latter.

Description Use the **display mac-authentication** command to display global MAC authentication information or MAC authentication information about specified ports.

Example # Display global MAC authentication information.

```
<Sysname> display mac-authentication
MAC address authentication is enabled.
User name format is MAC address, like xxxxxxxxxxxx
 Fixed username:mac
 Fixed password:not configured
         Offline detect period is 300s
         Quiet period is 60.
          Server response timeout value is 100s
         the max allowed user number is 1024 per slot
         Current user number amounts to 0
         Current domain: not configured, use default domain
Silent Mac User info:
         MAC ADDR               From Port           Port Index
Ethernet1/1 is link-up
  MAC address authentication is Enabled
  Authenticate success: 0, failed: 0
  Current online user number is 0
MAC ADDR         Authenticate state           AuthIndex
```

Table 520 Description on the fields of the display mac-authentication command

Field	Description
MAC address authentication is Enabled	Whether MAC authentication is enabled
User name format is MAC address, like xxxxxxxxxxxx	The username is in format of MAC address, like xxxxxxxxxxx
Fixed username:	Fixed username
Fixed password:	Password of the fixed username
Offline detect period	Setting of the offline detect timer
Quiet period	Setting of the quiet timer
Server response timeout value	Setting of the server timeout timer
The max allowed user number	Maximum number of users the device supports
Current user number amounts to	Total number of online users
Current domain: not configured, use default domain	Currently used ISP domain
Silent Mac User info	Information on users who are kept silent after failing MAC authentication
Ethernet1/1 is link-up	Status of the link on port Ethernet 1/1
MAC address authentication is Enabled	Whether MAC authentication is enabled on port Ethernet 1/1
Authenticate success: 0, failed: 0	MAC authentication statistics, including the number of successful authentication attempts and that of unsuccessful authentication attempts
Current online user number	Number of online users on the port
MAC ADDR	Online user MAC address
Authenticate state	User status. Possible values are: ■ CONNECTING: The user is logging in. ■ SUCCESS: The user has passed the authentication. ■ FAILURE: The user failed the authentication. ■ LOGOFF: The user has logged off.
AuthIndex	Authenticator Index

mac-authentication

Syntax **mac-authentication** [**interface** *interface-list*]

undo mac-authentication [**interface** *interface-list*]

View System view/Ethernet interface view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range

defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **mac-authentication** command to enable MAC authentication globally or for one or more ports.

Use the **undo mac-authentication** command to disable MAC authentication globally or for one or more ports.

By default, MAC authentication is neither enabled globally nor enabled on any port.

Note that:

- In system view, if you provide the *interface-list* argument, the command enables MAC authentication for the specified ports; otherwise, the command enables MAC authentication globally. In Ethernet interface view, the command enables MAC authentication for the port without requiring the *interface-list* argument.
- You can configure MAC authentication parameters globally or for specified ports either before or after enabling MAC authentication. If no MAC authentication parameters are configured before MAC authentication is enabled globally, the default values are used.
- You can enable MAC authentication for ports before enabling it globally. However, MAC authentication begins to function only after you also enable it globally.

Example # Enable MAC authentication globally.

```
<Sysname> systme-view
[Sysname] mac-authentication
```

Or

```
<Sysname> systme-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] mac-authentication
```

mac-authentication domain

Syntax **mac-authentication domain** *isp-name*

undo mac-authentication domain

View System view

Parameter *isp-name*: ISP domain name, a case-insensitive string of 1 to 24 characters that cannot contain any forward slash (/), colon (:), asterisk (*), question mark (?), less-than sign (<), greater-than sign (>), or at-sign (@).

Description Use the **mac-authentication domain** command to specify the ISP domain for MAC authentication.

Use the **undo mac-authentication domain** command to restore the default.

By default, the default ISP domain (system) is used.

Example # Specify the ISP domain for MAC authentication as **domain1**.

```
<Sysname> systme-view
[Sysname] mac-authentication domain domain1
```

mac-authentication timer

Syntax **mac-authentication timer** { **offline-detect** *offline-detect-value* | **quiet** *quiet-value* | **server-timeout** *server-timeout-value* }

undo mac-authentication timer { **offline-detect** | **quiet** | **server-timeout** }

View System view

Parameter **offline-detect** *offline-detect-value*: Specifies the offline detect interval, in the range 60 to 65,535 seconds.

quiet *quiet-value*: Specifies the quiet period, in the range 1 to 3,600 seconds.

server-timeout *server-timeout-value*: Specifies the server timeout period, in the range 100 to 300 seconds.

Description Use the **mac-authentication timer** command to set the MAC authentication timers.

Use the **undo mac-authentication timer** command to restore the defaults.

By default, the offline detect interval is 300 seconds, the quiet period is 60 seconds, and the server timeout period is 100 seconds.

The following timers function in the process of MAC authentication:

- Offline detect timer: At this interval, the device checks to see whether an online user has gone offline. Once detecting that a user becomes offline, the device sends to the RADIUS server a stop accounting notice.
- Quiet timer: Whenever a user fails MAC authentication, the device does not initiate any MAC authentication of the user during such a period.
- Server timeout timer: During authentication of a user, if the device receives no response from the RADIUS server in this period, it assumes that its connection to the RADIUS server has timed out and forbids the user from accessing the network.

Related command: **display mac-authentication**.

Example # Set the server timeout timer to 150 seconds.

```
<Sysname> systme-view
[Sysname] mac-authentication timer server-timeout 150
```

mac-authentication user-name-format

Syntax **mac-authentication user-name-format** { **fixed** [**account** *name*] [**password** { **cipher** | **simple** } *password*] | **mac-address** [**with-hyphen** | **without-hyphen**] }

undo mac-authentication user-name-format

View System view

Parameter **fixed**: Uses the MAC authentication username type of fixed username.

account *name*: Specifies the fixed username. The *name* argument is a case-insensitive string of 1 to 55 characters and defaults to mac.

password { **cipher** | **simple** } *password*: Specifies the fixed password for the fixed username. Using the **cipher** keyword displays the password in cipher text. Using the **simple** keyword displays the password in plain text. In the former case, the password can be either a string of 1 to 63 characters in plain text or a string of 24 or 88 characters in cipher text. In the latter case, the password must be a string of 1 to 63 characters in plain text.

mac-address: Adopts the user's source MAC address as the username, which is case-insensitive.

with-hyphen: Indicates that the MAC address must include "-", like xx-xx-xx-xx-xx-xx. The letters in the address must be in lower case.

without-hyphen: Indicates that the MAC address must not include "-", like xxxxxxxxxxxx. The letters in the address must be in lower case.

Description Use the **mac-authentication user-name-format** command to configure the username and password for MAC authentication.

Use the **undo mac-authentication user-name-format** command to restore the default.

By default, a user's source MAC address is used as the username and password. And whether "-" is necessary in the MAC address varies with devices.

Note that:

- When using the type of fixed username, you must also manually configure the password.
- When the user's source MAC address is used as the username, the password is also that MAC address.
- In cipher display mode, a password in plain text with no more than 16 characters will be encrypted into a password in cipher text with 24 characters,

and a password in plain text with 16 to 63 characters will be encrypted into a password in cipher text with 88 characters. For a password with 24 characters, the system will determine whether it can decrypt the password. If so, it treats the password as a cipher-text one. Otherwise, it treats it as a plain-text one.

Related command: **display mac-authentication**

Example # Configure the username for MAC authentication as **abc**, and the password displayed in plain text as **xyz**.

```
<Sysname> system-view
[Sysname] mac-authentication user-name-format fixed account abc pass
word simple xyz
```

reset mac-authentication statistics

Syntax **reset mac-authentication statistics** [**interface** *interface-list*]

View User view

Parameter **interface** *interface-list*: Specifies an Ethernet port list, in the format of { *interface-type interface-number* [**to** *interface-type interface-number*] }&<1-10>, where &<1-10> indicates that you can specify up to 10 port ranges. A port range defined without the **to** *interface-type interface-number* portion comprises only one port.

Description Use the **reset mac-authentication statistics** command to clear MAC authentication statistics.

Note that:

- If you do not specify the *interface-list* argument, the command clears the global MAC authentication statistics and the MAC authentication statistics on all ports.
- If you specify the *interface-list* argument, the command clears the MAC authentication statistics on the specified ports.

Related command: **display mac-authentication**.

Example # Clear MAC authentication statistics on Ethernet 1/0.

```
<Sysname> reset mac-authentication statistics interface ethernet 1/0
```

133 NAT CONFIGURATION COMMANDS

connection-limit default action

Syntax **connection-limit default action** [**permit** | **deny**]

undo connection-limit default action

View System view

Parameter **permit**: Enables the connection-limit function globally.

deny: Disables the connection-limit function globally.

Description Use the **connection-limit default action** command to specify the default connection-limit action globally, either permit or deny. The effect of this command applies to all user connections not defined in the connection-limit policy.

Use the **undo connection-limit default** command to restore the default.

By default, connection-limit is not enabled.

Example # Configure the default connection-limit action as permit.

```
<Sysname> system-view
[Sysname] connection-limit default action permit
```

connection-limit default amount

Syntax **connection-limit default amount** { **upper-limit** *max-amount* | **lower-limit** *min-amount* } *

undo connection-limit default amount

View System view

Parameter **upper-limit** *max-amount*: Specifies the upper limit of connections, in the range 1 to 4294967295.

lower-limit *min-amount*: Specifies the lower limit of connections, a value smaller than the upper limit, in the range 0 to 4294967295.

Description Use the **connection-limit default amount** command to set the limit(s) of user connections globally.

Use the **undo connection-limit default amount** command to restore the default.

By default, the upper limit is 100 and the lower limit is 20.

Example # Configure the upper limit as 200 and lower limit as 50.

```
<Sysname> system-view
[Sysname] connection-limit default amount upper-limit 200 lower-limit 50
```

connection-limit enable

Syntax **connection-limit enable**

undo connection-limit enable

View System view

Parameter None

Description Use the **connection-limit enable** command to enable the connection-limit function.

Use the **undo connection-limit enable** command to disable this function.

By default, the connection-limit function is disabled.

Once this function is enabled, both the connection number and the connection rate are limited.

Example # Enable the connection-limit function.

```
<Sysname> system-view
[Sysname] connection-limit enable
```

connection-limit policy

Syntax **connection-limit policy** *policy-number*

undo connection-limit policy { *policy-number* | **all** }

View System view

Parameter *policy-number*: Connection-limit policy number, in the range 0 to 19.

all: Deletes all connection-limit policies.

Description Use the **connection-limit policy** command to create or edit a connection-limit policy and enter connection-limit policy view.

Use the **undo connection-limit policy** command to delete a specified or all connection-limit policies.

Note that:

- A connection-limit policy contains a set of rules that define the connection-limit mode, the maximum connection rate and the connection number. By default, the connection-limit mode and the maximum connection rate are subject to the global configuration.
- When creating a connection-limit policy, you need to assign it a number that uniquely identifies that policy. Polices are matched by number in descending order.
- You can modify the rules in a policy only before binding the policy to a NAT module. No matter a connection-limit policy is bound to a NAT module or not, however, you can modify the connection-limit mode and the maximum connection rate. Additionally, you can add or delete rules to/from the policy.

Example # Create a connection-limit policy numbered 1.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
```

display connection-limit policy

Syntax **display connection-limit policy** { *policy-number* | **all** }

View Any view

Parameter *policy-number*: Number of a connection-limit policy, in the range 0 to 19.

all: Displays all connection-limit policies.

Description Use the **display connection-limit policy** command to display the information of a specified or all connection-limit policies.

Example # Display all connection-limit policies configured.

```
<Sysname> display connection-limit policy all
There is 1 policy:
Connection-limit policy 1, refcount 0 , 1 limit
 limit mode amount
 limit rate 11
 limit 1 acl 2001 per-source amount 1111 10
```

Table 521 Description on the fields of the display connection-limit policy all command

Field	Description
Connection-limit policy	Number of the connection-limit policy
refcount	Number of times that a policy is referenced

Table 521 Description on the fields of the display connection-limit policy all command

Field	Description
limit	Number of rules in the policy
limit mode	Connection-limit mode (all, amount, rate): ■ all: limits both connection number and connection rate. ■ amount: limits connection number only. ■ rate: limits connection rate only.
limit rate	Connection rate limit
acl	Access control list
per-source	Statistics based on the source addresses in the ACL
amount	Upper and lower limits of connections

display connection-limit statistics

Syntax **display connection-limit statistics** [**source** *src-address* { *mask* | *mask-length* }] [**destination** *dst-address* { *mask* | *mask-length* }] [**destination-port** { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*] [**vpn-instance** *vpn-instance-name*]

View Any view

Parameter **source** *src-address*: Displays the connection-limit statistics for the specified source address.

destination *dst-address*: Displays the connection-limit statistics for the specified destination address.

mask: Network mask.

mask-length: Mask length, in the range 1 to 32.

destination-port { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*: Displays connection-limit statistics based on the destination port number. You can specify the port(s) in different ways through different keywords: **eq** (equal to the specified port number), **gt** (greater than the specified port number), **lt** (less than the specified port number), **neq** (not equal to the specified port number), **range** (in a port range). The value range of *port-number* is 0 to 65,535. The value range of *start-port* and *end-port* is also 0 to 65,535, and the *start-port* must be not greater than the *end-port*.

vpn-instance *vpn-instance-name*: Specifies the MPLS VPN instance that a connection belongs to. The *vpn-instance-name* argument ranges from 1 to 19 characters. Absence of this keyword and argument indicates that the user whose connection statistics are to be displayed belongs to a normal private network rather than an MPLS VPN instance.

Description Use the **display connection-limit statistics** command to display connection-limit statistics.

Example # Display connection-limit statistics.

```
<Sysname> display connection-limit statistics
      source-ip       dest-ip         dest-port       vpn-instance
      192.168.0.210   ---             ---             ---
-------------------------------------------------------------------------
 NAT       amount         upper-limit    lower-limit    limit-flag
           2              200            100            0

      source-ip       dest-ip         dest-port       vpn-instance
      192.168.0.210   ---             ---             ---
-------------------------------------------------------------------------
 NAT       amount         upper-limit    lower-limit    limit-flag
           2              50             20             0
```

Table 522 Description on the fields of the display connection-limit statistics command

Field	Description
source-ip	Source IP address
dest-ip	Destination IP address
dest-port	Destination port number
vpn-instance	Name of the MPLS VPN instance that a connection belongs to
amount	Number of connections allowed to establish
upper-limit	Upper limit of connections
lower-limit	Lower limit of connections
limit-flag	Whether new connections are allowed, 0 means yes, 1 means no

display nat address-group

Syntax **display nat address-group**

View Any view

Parameter None

Description Use the **display nat address-group** command to display the NAT address pool information.

Example # Display the NAT address pool information.

```
<Sysname> display nat address-group
NAT address-group information:
  There are currently 1 nat address-group(s)
      1 : from         202.110.10.10   to         202.110.10.15
```

Table 523 Description on the fields of the display nat address-group command

Field	Description
NAT address-group information	NAT address pool information
There are currently 1 nat address-group(s)	There is one NAT address group
1 : from 202.110.10.10 to 202.110.10.15	The range of IP addresses in address pool 1 is from 202.110.10.10 to 202.110.10.15

display nat aging-time

Syntax **display nat aging-time**

View Any view

Parameter None

Description Use the **display nat aging-time** command to display the aging time values of different NAT sessions.

Example # Display the aging time values of different NAT sessions.

```
<Sysname> display nat aging-time
NAT aging-time value information:
       tcp ---- aging-time value is  86400 (seconds)
       udp ---- aging-time value is    300 (seconds)
      icmp ---- aging-time value is     60 (seconds)
      pptp ---- aging-time value is  86400 (seconds)
       dns ---- aging-time value is     60 (seconds)
   tcp-fin ---- aging-time value is     60 (seconds)
   tcp-syn ---- aging-time value is   3600 (seconds)
  ftp-ctrl ---- aging-time value is   7200 (seconds)
  ftp-data ---- aging-time value is    300 (seconds)
```

Table 524 Description on the fields of the display nat aging-time command

Field	Description
NAT aging-time value information	NAT aging time values for various protocols
tcp ---- aging-time value is 86400 (seconds)	NAT aging time for TCP is 86,400 seconds.
udp ---- aging-time value is 300 (seconds)	NAT aging time for UDP is 300 seconds.
icmp ---- aging-time value is 60 (seconds)	NAT aging time for ICMP is 60 seconds.
pptp ---- aging-time value is 86400 (seconds)	NAT aging time for PPTP is 86,400 seconds.
dns ---- aging-time value is 60 (seconds)	NAT aging time for DNS is 60 seconds.
tcp-fin ---- aging-time value is 60 (seconds)	NAT aging time for TCP fin or rst is 60 seconds.
tcp-syn ---- aging-time value is 3600 (seconds)	NAT aging time for TCP syn is 3,600 seconds.
ftp-ctrl ---- aging-time value is 7200 (seconds)	NAT aging time for FTP ctrl is 7,200 seconds.
ftp-data ---- aging-time value is 300 (seconds)	NAT aging time for FTP data is 300 seconds.

display nat all

Syntax **display nat all**

View Any view

Parameter None

Description Use the **display nat all** command to display the configurations of all NAT parameters.

Example # Display the configurations of all NAT parameters.

```
<Sysname> display nat all
  NAT address-group information:
There are currently 1 nat address-group(s)
      1 : from   202.110.10.10   to   202.110.10.15
NAT outbound information:
  There are currently 2 nat outbound rule(s)
                    Ethernet1/0: acl (2001) --- NAT address-group(1) [no-pat]
                    Ethernet2/0:          --- static
Server in private network information:
  There are currently 1 internal server(s)
  Interface:Ethernet1/0, Protocol:6(tcp),
     [global]    202.110.10.10:      8080   [local]     10.110.10.10:   80(www)
NAT static information:
  There are currently 2 static table(s)
        GlobalAddr          InsideAddr         Vpn-instance
  192.168.1.111              2.3.4.5           ----
        4.4.4.4              3.3.3.3           ----
NAT aging-time value information:
       tcp ---- aging-time value is  86400 (seconds)
       udp ---- aging-time value is    300 (seconds)
      icmp ---- aging-time value is     60 (seconds)
      pptp ---- aging-time value is  86400 (seconds)
       dns ---- aging-time value is     60 (seconds)
   tcp-fin ---- aging-time value is     60 (seconds)
   tcp-syn ---- aging-time value is   3600 (seconds)
  ftp-ctrl ---- aging-time value is   7200 (seconds)
  ftp-data ---- aging-time value is    300 (seconds)
NAT log information:
  log enable  :  enable acl 2000
  flow-begin  :  enable
  flow-active :  10(minutes)
```

Table 525 Description on some fields of the display nat all command

Field	Description
NAT address-group information	NAT address pool information
1 : from 202.110.10.10 to 202.110.10.15	The IP address range of address pool 1 is from 202.110.10.10 to 202.110.10.15
NAT outbound information:	Configuration information about internal address-to-external address translation
Ethernet1/0: ACL(2001) --- NAT address-group(1) [no-pat]	On interface Ethernet 1/0, ACL 2001 is associated with address pool 1 to provide many-to-many address translation. [no-pat] indicates that port address is not translated.
Ethernet2/0: --- static	Static NAT is configured on Ethernet 2/0.
Server in private network information	Information of internal servers

Table 525 Description on some fields of the display nat all command

Field	Description
Interface:Ethernet1/0, Protocol:6(tcp), [global] 202.110.10.10: 8080 [local] 10.110.10.10: 80(www)	An internal server, a WWW server, is configured on interface Ethernet 1/0. Its internal address and port number are 10.110.10.10 and 80 respectively. Its external address and port number are 202.110.10.10 and 8080 respectively. The protocol used is TCP.
NAT static information:	Information about static NAT:
There are currently 2 static table(s)	There are currently 2 static NAT entries.
GlobalAddr	External IP address
InsideAddr	Internal IP address
Vpn-instance	Layer 3 VPN to which the internal IP address belongs
tcp ---- aging-time value is 86400 (seconds)	The aging time for TCP is 86,400 seconds.
udp ---- aging-time value is 300 (seconds)	The aging time for UDP is 300 seconds.
icmp ---- aging-time value is 60 (seconds)	The aging time for ICMP is 60 seconds.
pptp ---- aging-time value is 86400 (seconds)	The aging time for PPTP is 86,400 seconds.
dns ---- aging-time value is 60 (seconds)	The aging time for DNS is 60 seconds.
tcp-fin ---- aging-time value is 60 (seconds)	The aging time for TCP fin or rst is 60 seconds.
tcp-syn ---- aging-time value is 3600 (seconds)	The aging time for TCP syn is 3,600 seconds.
ftp-ctrl ---- aging-time value is 7200 (seconds)	The aging time for FTP ctrl is 7,200 seconds.
ftp-data ---- aging-time value is 300 (seconds)	The aging time for FTP data is 300 seconds.
NAT log information:	NAT log information
log enable: enable acl 2000	Logging data flows matching acl 2000
flow-begin: enable	Logging newly established sessions
flow-active: 10(minutes)	Interval in logging active flows (10 minutes)

display nat connection-limit

Syntax **display nat connection-limit** [**source** *src-address* { *mask* | *mask-length* }] [**destination** *dst-address* { *mask* | *mask-length* }] [**destination-port** { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*] [**vpn-instance** *vpn-instance-name*]

View Any view

Parameter **source** *src-address*: Displays the connection-limit statistics of a specified source address.

destination *dst-address*: Displays the connection-limit statistics of a specified destination address.

mask: Network mask.

mask-length: The length of net mask, in the range 1 to 32.

destination-port { **eq** | **gt** | **lt** | **neq** | **range** } *port-number*: Displays connection-limit statistics based on the destination port number. You can specify the port(s) in different ways through different keywords: **eq** (equal to the specified port number), **gt** (greater than the specified port number), **lt** (less than the specified port number), **neq** (not equal to the specified port number), **range** (port range). The value range of *port-number* is 0 to 65,535. The value range of *start-port* and *end-port* is also 0 to 65,535, and the *start-port* must be not bigger than the *end-port*.

vpn-instance *vpn-instance-name*: Specifies the MPLS VPN instance that a connection belongs to. The *vpn-instance-name* argument ranges from 1 to 31 characters. Absence of this keyword and argument indicates that the user whose connection statistics are to be displayed belongs to a normal private network rather than an MPLS VPN instance.

Description Use the **display nat connection-limit** command to display NAT connection-limit statistics.

Example # Display NAT connection-limit statistics.

```
<Sysname> display nat connection-limit
      source-ip       dest-ip         dest-port       vpn-instance
      192.168.0.210   ---             ---             ---
------------------------------------------------------------------------------
 NAT       amount         upper-limit    lower-limit    limit-flag
           2              50             20             0
```

Table 526 Description on the fields of the display nat connection-limit command

Field	Description
source-ip	Source IP address of the connection. "---" indicates that the value is not available.
dest-ip	Destination IP address of the connection. "---" indicates that the value is not available.
dest-port	Destination port of the connection. "---" indicates that the value is not available.
vpn-instance	MPLS VPN instance that a connection belongs to. "---" indicates that the connection does not belong to any MPLS VPN instance.
NAT	Indicates that the connection is created through NAT
amount	Number of active connections
upper-limit	Upper limit of connections
lower-limit	Lower limit of connections
limit-flag	Whether new connections are allowed to establish: 0 means yes, 1 means no

display nat log

Syntax **display nat log**

View Any view

Parameter None

Description Use the **display nat log** command to view the NAT log configuration.

Example # View the NAT log configuration.

```
<Sysname> display nat log
NAT log information:
  log enable  :  enable acl 2000
  flow-begin  :  enable
  flow-active :  10(minutes)
```

Table 527 Description on the fields of the display nat log command:

Field	Description
NAT log information :	NAT log configuration
log enable : enable acl 2000	Logging data flows matching acl 2000.
flow-begin : enable	Logging newly established sessions
flow-active : 10(minutes)	Interval in logging active flows (10 minutes)

display nat outbound

Syntax **display nat outbound**

View Any view

Parameter None

Description Use the **display nat outbound** command to display the address translation information.

Example # Display the NAT address translation information.

```
<Sysname> display nat outbound
NAT outbound information:
  There are currently 2 nat outbound rule(s)
                  Ethernet1/0: acl(2001) --- NAT address-group(1) [no-pat]
                  Ethernet1/1: acl(2002) --- interface
```

Table 528 Description on the fields of the display nat outbound command

Field	Description
NAT outbound information:	Display configured NAT address translation information
Ethernet1/0: acl(2001) --- NAT address-group(1) [no-pat]	ACL 2001 is associated with address pool 1 on interface Ethernet 1/0 to provide many-to-many NAT. [no-pat] indicates that port address is not translated.
Ethernet1/1: acl(2002) --- interface	ACL 2002 is associated with interface Ethernet 1/1 to implement Easy IP

display nat server

Syntax **display nat server**

View Any view

Parameter None

Description Use the **display nat server** command to display information about internal servers.

Example # Display information about internal servers.

```
<Sysname> display nat server
Server in private network information:
  There are currently 1 internal server(s)
  Interface: Ethernet1/0, Protocol: 6(tcp),
     [global]    202.110.10.10:      8080   [local]     10.110.10.10:   80(www)
```

Table 529 Description on the fields of the display nat server command

Field	Description
Server in private network information	Information about internal servers
Interface:Ethernet1/0, Protocol:6(tcp), [global] 202.110.10.10: 8080 [local] 10.110.10.10: 80(www)	On interface Ethernet 1/0, a WWW server is configured. Its internal address and port number are 10.110.10.10 and 80, respectively. Its external address and port number are 202.110.10.10 and 8080, respectively. The protocol type is TCP.

display nat session

Syntax **display nat session** [**vpn-instance** *vpn-instance-name*] [**source** { **global** *global-address* | **inside** *inside-address* }] [**destination** *dst-address*]

View Any view

Parameter **vpn-instance** *vpn-instance-name*: Displays NAT translation table entries in the specified MPLS VPN instance. The *vpn-instance-name* is a string of 1 to 31 characters.

source global *global-address*: Displays NAT translation table entries for the specified external source IP address.

source inside *inside-address*: Displays NAT translation table entries for the specified internal source IP address.

destination *dst-address*: Displays NAT translation table entries for the specified destination IP address.

Description Use the **display nat session** command to display the active NAT sessions.

Example # Display the active NAT sessions.

```
<Sysname> display nat session
There are currently 1 NAT session:

Protocol      GlobalAddr  Port      InsideAddr  Port        DestAddr  Port
       1        2.2.2.10 12288   192.168.0.210   768         2.2.2.2   768
 VPN:  0,        status:  4011,        TTL: 00:01:00,       Left: 00:00:53
```

Table 530 Description on the fields of the display nat session command

Field	Description
Protocol	Protocol number. 1 represents ICMP.
GlobalAddr Port	External IP address and port number after translation
InsideAddr Port	Internal IP address and port number before translation
DestAddr Port	Destination IP address and port number
VPN	Index of the MPLS VPN instance to which translation table entries belong. Its value varies from system to system. For systems that support 1,024 VPN instances, this parameter ranges from 0 to 1,023. A value of 0 indicates that translation table entries do not belong to any MPLS VPN instance.
status	Status of translation table entries
TTL	Lifetime of translation table entries, in the format of hh:mm:ss
Left	Remaining lifetime of translation table entries, in the format of hh:mm:ss

display nat statistics

Syntax **display nat statistics**

View Any view

Parameter None

Description Use the **display nat statistics** command to display NAT statistics.

Example # Display NAT statistics.

```
<Sysname> display nat statistics
  total PAT session table count: 0
  total NO-PAT session table count: 0
  total SERVER session table count: 0
  total STATIC session table count: 0
  total FRAGMENT session table count: 0
  total session table count HASH by Internet side IP: 0

  active PAT session table count: 0
  active NO-PAT session table count: 0
  active FRAGMENT session table count: 0
  active session table count HASH by Internet side IP: 0
```

Table 531 Description on the fields of the display nat statistics command

Field	Description
total PAT session table count	Number of PAT session entries

Table 531 Description on the fields of the display nat statistics command

Field	Description
total NO-PAT session table count	Number of No-PAT session entries
total SERVER session table count	Number of SERVER session entries
total STATIC session table count	Number of STATIC session entries
total FRAGMENT session table count	Number of FRAGRANT session entries
total session table count HASH by Internet side IP	Number of HASH entries calculated based upon the external IP address
active PAT session table count	Number of active PAT session entries
active NO-PAT session table count	Number of active No-PAT session entries
active FRAGMENT session table count	Number of active FRAGRANT session entries
active session table count HASH by Internet side IP	Number of active HASH entries calculated based upon the external IP address

display userlog export

Syntax **display userlog export**

View Any view

Parameter None

Description Use the **display userlog export** command to view the configuration and statistics of NAT logs for a card.

Related command: **reset userlog export**

Example # View the configuration and statistics of NAT logs.

```
<Sysname> display userlog export
NAT:
   No ip userlog export is enabled
```

limit acl

Syntax **limit** *limit-id* **acl** *acl-number* [**per-destination** | **per-service** | **per-source**] * **amount** *max-amount min-amount*

undo limit *limit-id*

View Connection-limit policy view

Parameter *limit-id*: ID for a rule in a connection-limit policy, an integer in the range 0 to 255.

acl-number: Number for an ACL, in the range 2,000 to 3,999. Only data flows that match this ACL are limited.

per-destination: Limits connections based upon the destination address.

per-service: Limits connections based upon the service type.

per-source: Limits connections based upon the source address.

amount: Limits the number of connections.

max-amount: Maximum connection number, in the range 1 to 4294967295

min-amount: Minimum connection number, a value smaller than the upper limit, in the range 0 to 4294967295.

Description Use the **limit acl** command to configure a rule in a connection-limit policy.

Use the **undo limit** command to remove the configuration

Example # Configure connection-limit policy 1. Set the maximum and minimum number of connections to a destination IP address 1.1.1.1 as 200 and 100 respectively. Configure ACL 2001, defining that only connections initiated from 192.168.0.0/24 are limited. This means that the number of user connections which initiated from 192.168.0.0/24 and connecting to public server 1.1.1.1 cannot exceed 200.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 192.168.0.0 0.0.0.255
[Sysname-acl-basic-2001] quit
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] limit 1 acl 2001 per-destination
 amount 200 100
```

limit mode

Syntax **limit mode amount**

undo limit mode

View Connection-limit policy view

Parameter None

Description Use the **limit mode amount** command to specify a connection-limit mode.

Use the **undo limit mode** command to remove the configuration and restore the default.

By default, the connection number is limited.

Example # Specify a connection-limit mode for connection-limit policy 1.

```
<Sysname> system-view
[Sysname] connection-limit policy 1
[Sysname-connection-limit-policy-1] limit mode amount
```

nat address-group

Syntax **nat address-group** *group-number start-address end-address*

undo nat address-group *group-number*

View System view

Parameter *group-number*: Index of an address pool, in the range 0 to 31.

start-address: The beginning IP address in an address pool.

end-address: The ending IP address in an address pool.

Description Use the **nat address-group** command to specify an address pool for NAT.

Use the **undo nat address-group** command to remove the configuration.

An address pool is a set of continuous IP addresses. When an internal packet is forwarded to the external network, the system selects an address from the pool to serve as the source address after address translation. An equal *start-address* and *end-address* means there is only one IP address in the address pool.

Note that:

- You cannot delete an address pool which has been associated with an ACL.
- An address pool is not needed in the case of Easy IP where the interface's public IP address is used as the translated IP address.

- *The volume of an address pool (that is, the number of addresses contained) varies by device models.*
- *For some devices, the addresses in their address pools cannot include the addresses in the normal address pool, the public IP address of interface in the case of Easy IP or that of the internal server.*

Example # Configure an address pool numbered 1 that contains addresses 202.110.10.10 to 202.110.10.15.

```
<Sysname> system-view
[Sysname] nat address-group 1 202.110.10.10 202.110.10.15
```

nat aging-time

Syntax **nat aging-time** { **default** | { **dns** | **ftp-ctrl** | **ftp-data** | **icmp** | **pptp** | **tcp** | **tcp-fin** | **tcp-syn** | **udp** } *seconds* }

View System view

Parameter **default**: Restores the NAT aging time to the default value.

dns: Specifies the NAT aging time for DNS, which defaults to 60 seconds.

ftp-ctrl: Specifies the NAT aging time for FTP control link, which defaults to 7,200 seconds.

ftp-data: Specifies the NAT aging time for FTP data link, which defaults to 300 seconds.

icmp: Specifies the NAT aging time for ICMP, which defaults to 60 seconds.

pptp: Specifies the NAT aging time for PPTP, which defaults to 86,400 seconds.

tcp: Specifies the NAT aging time for TCP, which defaults to 86,400 seconds.

tcp-fin: Specifies the NAT aging time for TCP fin or rst, which defaults to 60 seconds.

tcp-syn: Specifies the NAT aging time for TCP syn, which defaults to 3,600 seconds.

udp: Specifies the NAT aging time for UDP, which defaults to 300 seconds.

seconds: NAT aging time, in the range 10 to 86,400 seconds (24 hours).

Description Use the **nat aging-time** command to configure NAT aging time(s).

The Hash table used in address translation is not permanent. This command configures a Hash table life time for TCP, UDP, ICMP, and other protocols respectively. If the Hash table is not used within the configured time, the Hash entry will become invalid. For example, when a user with IP address 10.110.10.10 and port number 2000 establishes an external TCP connection, NAT will assign an IP address and a port number for the user. If, within a preconfigured aging time, the TCP connection is not used, the system will remove it.

Example # Configure the NAT aging time for TCP to be 240 seconds.

```
<Sysname> system-view
[Sysname] nat aging-time tcp 240
```

nat alg

Syntax **nat alg** { **dns** | **ftp** | **ils** | **nbt** | **pptp** }

undo nat alg { **dns** | **ftp** | **ils** | **nbt** | **pptp** }

View System view

Parameter **dns**: Supports DNS.

ftp: Supports FTP.

ils: Supports ILS.

nbt: Supports NBT.

pptp: Supports PPTP.

Description Use the **nat alg** command to enable NAT application layer gateway for the specified protocol.

Use the **undo nat alg** command to disable NAT application layer gateway.

By default, NAT application layer gateway is enabled.

Example # Enable NAT application layer gateway for FTP.

```
<Sysname> system-view
[Sysname] nat alg ftp
```

nat connection-limit-policy

Syntax **nat connection-limit-policy** *policy-number*

undo nat connection-limit-policy *policy-number*

View System view

Parameter *policy-number*: Number of the connection-limit policy to be bound with the NAT module. The value ranges from 0 to 19.

Description Use the **nat connection-limit-policy** command to bind a connection-limit policy with the NAT module.

Use the **undo nat connection-limit-policy** command to remove the configuration.

Note that:

- A NAT module can be bound with only one policy.
- The globally configured connection limits are not effective unless a connection-limit policy is bound to the NAT module.
- If there are multiple NAT boards, the configuration applies to all the boards.

Example # Bind connection-limit policy 1 with the NAT module.

```
<Sysname> system-view
[Sysname]nat connection-limit-policy 1
```

Remove the binding between connection-limit policy 1 and the NAT module.

```
<Sysname> system-view
[Sysname]undo nat connection-limit-policy 1
```

nat log enable

Syntax **nat log enable** [**acl** *acl-number*]

undo nat log enable

View System view

Parameter **acl** *acl-number*: Enables the NAT log function for the data flows that match the specified ACL. The *acl-number* parameter ranges from 2,000 to 3,999. Absence of this parameter indicates that NAT log function applies to all data flows.

Description Use the **nat log enable** command to enable the NAT log function.

Use the **undo nat log enable** command to disable the NAT log function.

By default, the NAT log function is disabled.

Example # Enable the NAT log function.

```
<Sysname> system-view
[Sysname] nat log enable acl 2001
```

Disable the NAT log function.

```
<Sysname> system-view
[Sysname] undo nat log enable
```

nat log flow-active

Syntax **nat log flow-active** *minutes*

undo nat log flow-active

View System view

Parameter *minutes*: Interval in logging the active NAT sessions, in the range 10 to 120 minutes.

Description Use the **nat log flow-active** command to enable logging for NAT active sessions and specify the interval in creating and sending the logs.

Use the **undo nat log flow-active** command to disable this function.

By default, this function is disabled.

This command allows you to log active flows regularly. This solves the problem of logging long-last active sessions as logs are normally generated only when a session is established or deleted.

Example # Configure the interval between sending NAT active-flow logs as 10 minutes.

```
<Sysname> system-view
[Sysname] nat log flow-active 10
```

Delete the configured interval.

```
<Sysname> system-view
[Sysname] undo nat log flow-active
```

nat log flow-begin

Syntax **nat log flow-begin**

undo nat log flow-begin

View System view

Parameter None

Description Use the **nat log flow-begin** command to generate NAT logs while establishing a NAT session.

Use the **undo nat log flow-begin** command to restore the default.

By default, no log is generated when establishing a session.

Example # Generate NAT log while establishing a session.

```
<Sysname> system-view
[Sysname] nat log flow-begin
```

nat outbound

Syntax **nat outbound** *acl-number* [**address-group** *group-number* [**no-pat**]]

undo nat outbound *acl-number* [**address-group** *group-number* [**no-pat**]]

View Interface view

Parameter **address-group**: Specifies an address pool for NAT. If no address pool is specified, the interface IP address will be used, that is, the Easy IP feature.

acl-number: ACL (including both the basic and the advanced) number, in the range 2,000 to 3,999.

group-number: Number of a predefined address pool. The value range varies by device models.

no-pat: Translates IP addresses only, without dealing with the port information.

Description

Use the **nat outbound** command to enable NAT and associate an ACL with an address pool. Packets that match the ACL rules will have their internal IP address replaced by an address from the address pool.

Use the **undo nat outbound** command to remove the association.

Note that:

- You can configure different associations on one interface. Normally, the associations are configured on the egress interface of an internal network that connects to the external network(s).
- In the case of Easy IP, if you have modified the interface address, you must reset the original NAT translation table using the **reset nat session** command before accessing external networks. Otherwise, it is possible that the original NAT table entries cannot be automatically deleted or deleted with the **reset nat** command.
- Once the **undo nat outbound** command is executed, the NAT translation table entries generated by the **nat outbound** command will not be deleted. They will be aged out automatically after 5 to 10 minutes. During this period, users who use these table entries cannot access external networks whereas other users are not affected. You can also use the **reset nat session** command to clear all the NAT address translation table entries. However, use of this command will result in termination of address translation and all users will have to reestablish connections. Users can make a proper choice as required.
- When an ACL rule is not operative, no new NAT session entry depending on the rule can be created. However, an existing connection is still available for communication.

The following restrictions exist for some devices

- *The ACL rules referenced by the same interface cannot conflict. That is, the source IP address, destination IP address and VPN instance information in any two ACL rules cannot be the same. For basic ACLs (2,000 to 2,999), if the source IP address and VPN instance information in any two ACL rules are the same, a conflict occurs.*
- *EASY IP cannot be configured on interface configured with DHCP Client.*
- *An address pool must be configured on just one VLAN interface.*

Example

Enable NAT for hosts in the 10.110.10.0/24 segment, using addresses 1.10.10.1 to 1.10.10.20 as the external IP addresses. Assume that interface Serial 1/0 is connected to the external network.

```
<Sysname> system-view
[Sysname] acl number 2001
[Sysname-acl-basic-2001] rule permit source 10.110.10.0 0.0.0.255
[Sysname-acl-basic-2001] rule deny
[Sysname-acl-basic-2001] quit
```

Configure the address pool.

```
[Sysname] nat address-group 1 1.10.10.1 1.10.10.20
```

Enable NAT. Use the IP addresses from address pool 1 while dealing with TCP/UDP port information.

```
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat outbound 2001 address-group 1
```

If you do not deal with the TCP/UDP port information, do the following:

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat outbound 2001 address-group 1 no-pat
```

To use the IP address of the Serial 1/0 interface for address translation, do the following:

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat outbound 2001
```

nat outbound static

Syntax **nat outbound static**

undo nat outbound static

View Interface view

Parameter None

Description Use the **nat outbound static** command to enable on an interface the one-to-one (static) NAT configured with the **nat static** command.

Use the **undo nat outbound static** command to cancel the one-to-one (static) NAT on the interface.

Example # Configure one-to-one NAT and enable this NAT on interface Serial 2/0.

```
<Sysname> system-view
[Sysname] nat static 192.168.1.1 2.2.2.2
[Sysname] serial 1/0
[Sysname-Serial1/0] nat outbound static
```

nat server

Syntax **nat server** [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-address* | **interface** { *interface-type interface-number* } | **current-interface** } *global-port1 global-port2* **inside** *host-address1 host-address2 host-port*

nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-address* | **interface** { *interface-type interface-number*} | **current-interface** } [*global-port*] **inside** *host-address* [*host-port*]

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-address* | **interface** { *interface-type interface-number*} | **current-interface** } *global-port1 global-port2* **inside** *host-address1 host-address2 host-port*

undo nat server [**vpn-instance** *vpn-instance-name*] **protocol** *pro-type* **global** { *global-address* | **interface** { *interface-type interface-number*} | **current-interface** } [*global-port*] **inside** *host-address* [*host-port*]

View Interface view

Parameter *vpn-instance-name*: Instance name of a VPN to which an internal server belongs, in the range 1 to 31 characters. Absence of this parameter indicates that the internal server belongs to a normal private network instead of an MPLS VPN instance.

pro-type: Type of protocols over IP. It could be provided either in protocol number or key word, such as **icmp** (or its protocol number 1), **tcp** (or 6), **udp** (or 17). The value ranges from 1 to 255.

global-address: A valid IP address designated for external access.

interface: Uses a specified interface address as the public IP address of an internal server. This only applies to Easy IP.

interface-type interface-number: Specifies the interface type and interface number. Currently, this interface must be an existing Loopback interface.

current-interface: Uses the current interface address as the public IP address of an internal server.

global-port1, global-port2: Jointly specifies a port range that corresponds to the IP address range of internal hosts. Note that *global-port2* must be greater than *global-port1*.

host-address1, host-address2: Jointly defines a sequence of addresses that corresponds to the port range. Note that *host-address2* must be greater than *host-address1* and that the range and number of the addresses must match those of the ports.

host-port: Port number provided by the NAT server, in the range 0 to 65,535. The default value is 0, suggesting a static connection between the *global-address* and *host-address.*

- You can use the service names (or keywords) to represent those well-known port numbers, for example, you can use **www** to represent port number 80, **ftp** to represent port number 21, and so on.
- In particular, you can use the keyword **any** to represent port number 0, which means all types of services are supported.
- The support for a default port number varies by device models.

global-port: Port number designated for external access, in the range 0 to 65,535. The default and the keyword must match those for *host-port.*

host-address: Internal IP address of the NAT server.

Description Use the **nat server** command to define a translation table for an internal server.

Using the address and port combination defined by the *global-address* and *global-port* parameters, external users can access internal servers with an IP address of *host-address* and a port of *host-port*.

Use the **undo nat server** command to remove the configuration.

Note that:

- Of the two arguments *global-port* and *host-port*, if one is set to **any**, the other must also be **any**, or remain undefined.
- Using this command, you can configure internal servers (such as WWW, FTP, Telnet, POP3, or DNS server) that provide services to external users. An internal server can reside in a private network or in an MPLS VPN instance.
- An interface can be configured with at most 256 internal server configuration commands. Each command can create a number of internal servers equal to the difference between *global-port2* and *global-port1*. An interface can be configured with at most 4096 internal servers and a system allows at most 1024 internal server configuration commands.
- In general, this command is configured on the interface that serves as the egress of an internal network and connects to the external networks.
- Currently the device supports Easy IP, which uses the interface address as the public IP address of internal servers. To implement Easy IP on the current interface, use key word **current-interface** in the command. To implement Easy IP on other interfaces, you must specify an existing Loopback interface.

CAUTION: *When the protocol type is not* ***udp*** *(with a protocol number of 17) or* ***tcp*** *(with a protocol number of 6), you can only use the (****undo) nat server*** *[* ***vpn-instance*** *vpn-instance-name]* ***protocol*** *pro-type* ***global*** *global-address* ***inside*** *host-address command, that is, one-to-one NAT between an internal IP address and an external IP address.*

Example # Specify the IP address of the WWW Server in a LAN to be 10.110.10.10, the IP address of the FTP Server in MPLS VPN vrf10 to be 10.110.10.11. It is desired to allow external users to access the WWW Server through http:// 202.110.10.10:8080, and the FTP Server through ftp://202.110.10.10. Assume that the interface Serial 1/0 is connected to external networks.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat server protocol tcp global 202.110.10.10 808
0 inside 10.110.10.10 www
[Sysname-Serial1/0] quit
[Sysname] ip vpn-instance vrf10
[Sysname-vpn-instance] route-distinguisher 100:001
[Sysname-vpn-instance] vpn-target 100:1 export-extcommunity
[Sysname-vpn-instance] vpn-target 100:1 import-extcommunity
```

```
[Sysname-vpn-instance] quit
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat server vpn-instance vrf10 protocol tcp globa
l 202.110.10.10 inside 10.110.10.11
```

Specify a host with an IP address of 10.110.10.12 in VPN vrf10. An external host pings 202.110.10.11 to examine the connectivity to the host.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat server vpn-instance vrf10 protocol icmp glob
al 202.110.10.11 inside 10.110.10.12
```

Specify the external IP address as 202.110.10.10. Telnet the hosts which IP addresses range from 10.110.10.1 to 10.110.10.100 in MPLS VPN vrf10 through the ports ranging from 1001 to 1100, for example, telnet 10.110.10.1 from 202.110.10.10:1001, telnet 10.110.10.2 from 202.110.10.10:1002 and so on.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] nat server vpn-instance vrf10 protocol tcp globa
l 202.110.10.10 1001 1100 inside 10.110.10.1 10.110.10.100 telnet
```

Remove the WWW server using the following commands.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] undo nat server protocol tcp global 202.110.10.1
0 8070 inside 10.110.10.10 www
```

Remove the FTP server in VPN vrf10 using the following commands.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] undo nat server vpn-instance vrf10 protocol tcp
global 202.110.10.11 8070 inside 10.110.10.11 ftp
```

nat static

Syntax **nat static** { *ip-address1 ip-address2* | **net-to-net** *start-ip end-ip* **global** *global-net-address* { *mask* | *mask-length* } }

undo nat static { *ip-address1 ip-address2* | **net-to-net** *start-ip end-ip* **global** *global-net-address* { *mask* | *mask-length* } }

View System view

Parameter *ip-address1*: Internal IP address.

ip-address2: External IP address.

net-to-net: Specifies static translation for network segment mapping.

start-ip: Start address of an internal IP address range.

end-ip: End address of an internal IP address range. The end address must not be smaller than the start address.

Global: Specifies an external network address.

global-net-address: External network address.

Mask: External network mask.

mask-length: Length of the external network mask, in the range of 1 to 32.

Description Use the **nat static** command to configure static NAT between an internal IP address and an external IP address.

Use the **undo nat static** command to remove the configuration.

There are two ways to configure static NAT between an internal IP address and an external IP address:

- One-to-one NAT: An internal IP address is translated into an external IP address.
- Net-to-net NAT: The IP addresses of an internal network segment are mapped with the IP addresses of an external network segment.

Note that when configuring net-to-net NAT, you must ensure that internal IP addresses fall in one network segment when ANDed with the external network mask.

Example # Configure static NAT between 192.168.1.1 and 2.2.2.2.

```
<Sysname> system-view
[Sysname] nat static 192.168.1.1 2.2.2.2
```

Configure static NAT between the internal segment ranging 192.168.1.1 to 192.168.1.100 and the external segment 172.16.0/24.

```
<Sysname> system-view
[Sysname] nat static net-to-net 192.168.1.1 192.168.1.100 global 172
.16.0.0 255.255.255.0
```

reset nat session

Syntax **reset nat session**

View User view

Parameter None

Description Use the **reset nat session** command to clear the address translation table and release the memory for storing the table.

Example # Clear the address translation table.

```
<Sysname> reset nat session
```

reset userlog export

Syntax **reset userlog export**

View Use view

Parameter None

Description Use the **reset userlog export** command to clear the NAT log statistics.

Once the NAT log function is enabled, the system will make statistics for NAT logs periodically.

Related command: **display userlog export**

Example # Clear the NAT log statistics.

```
<Sysname> reset userlog export
```

reset userlog nat logbuffer

Syntax **reset userlog nat logbuffer**

View User view

Parameter None

Description Use the **reset userlog nat logbuffer** command to clear the NAT log buffer.

CAUTION: *Clearing the NAT log buffer will remove all NAT logs in the buffer. You are not recommended to use this command in normal situations.*

Example # Clear the NAT logs in the buffer.

```
<Sysname> reset userlog nat logbuffer
```

userlog nat export host

Syntax **userlog nat export host** *ip-address udp-port*

undo userlog nat export host

View System view

Parameter *ip-address*: IP address of the NAT log server. The address must be a valid unicast IP address and cannot be a loopback address.

udp-port: UDP port number of the NAT log server, ranging from 0 to 65535.

Description Use the **userlog nat export host** command to configure the IP address and UDP port number of the NAT log server that receives NAT logs.

Use the **undo userlog nat export host** command to restore the default setting.

By default, no IP address or UDP port number of the NAT log server is configured.

Note that:

- You must configure the NAT log server to successfully export NAT logs in UDP packets.
- You are recommended to use a UDP port number greater than 1024 to avoid conflicting with common UDP port numbers.

Related command: **userlog nat export source-ip**

Example # Export NAT logs to the NAT log server whose IP address is 169.254.1.1:2000.

```
<Sysname> system-view
[Sysname] userlog nat export host 169.254.1.1 2000
```

userlog nat export source-ip

Syntax **userlog nat export source-ip** *ip-address*

undo userlog nat export source-ip

View System view

Parameter *ip-address*: Source IP address of the exported UDP packets.

Description Use the **userlog nat export source-ip** command to set the source IP address of the UDP packets that carry NAT logs.

Use the **undo userlog nat export source-ip** command to restore the default.

By default, the source IP address of the UDP packets that carry NAT logs is the IP address of the interface that sends the UDP packets.

Related command: **userlog nat export host**.

Example # Set 169.254.1.2 as the source IP address of the UDP packets that carry NAT logs.

```
<Sysname> system-view
[Sysname] userlog nat export source-ip 169.254.1.2
```

userlog nat export version

Syntax **userlog nat export version** *version-number*

undo userlog nat export version

View System view

Parameter *version-number*: Version number of NAT logs. Currently, the system supports version 1 only.

Description Use the **userlog nat export version** command to set the version number of NAT logs.

Use the **undo userlog nat export version** command to restore the default.

By default, the version number of NAT logs is 1.

Example # Set the version number of NAT logs to 1.

```
<Sysname> system-view
[Sysname] userlog nat export version 1
```

userlog nat syslog

Syntax **userlog nat syslog**

undo userlog nat syslog

View System view

Parameter None

Description Use the **userlog nat syslog** command to export NAT logs to the information center.

Use the **undo userlog nat syslog** command to restore the default.

By default, NAT logs are exported to the NAT log server.

Note that as NAT logs may occupy large memory, it is not advisable to export large amount of NAT logs to the information center.

Example # Export NAT logs to the information center.

```
<Sysname> system-view
[Sysname] userlog nat syslog
```

134 PKI CONFIGURATION COMMANDS

attribute

Syntax **attribute** *id* { **alt-subject-name** { **fqdn** | **ip** } | { **issuer-name** | **subject-name** } { **dn** | **fqdn** | **ip** } } { **ctn** | **equ** | **nctn** | **nequ**} *attribute-value*

undo attribute { *id* | **all** }

View Certificate attribute group view

Parameter *Id*: Sequence number of the certificate attribute rule, in the range 1 to 16.

alt-subject-name: Specifies the name of the alternative certificate subject.

fqdn: Specifies the FQDN of the entity.

ip: Specifies the IP address of the entity.

issuer-name: Specifies the name of the certificate issuer.

subject-name: Specifies the name of the certificate subject.

dn: Specifies the domain name of the entity.

ctn: Specifies the contain operation.

equ: Specifies the equal operation.

nctn: Specifies the not-contain operation.

nequ: Specifies the not-equal operation.

attribute-value: Value of the certificate attribute, a case-insensitive string of 1 to 128 characters.

all: Specifies all certificate attributes.

Description Use the **attribute** command to configure the attribute rules of the certificate issuer name, certificate subject name and alternative certificate subject name.

Use the **undo attribute** command to delete the attributes of one or all certificates.

By default, there is no restriction on the issuer name, the subject name and the alternative subject name of a certificate.

Note that the attribute of the alternative certificate subject name does not appear as a domain name, and therefore the **dn** keyword is not available for the attribute.

Example # Create a certificate attribute rule, specifying that the DN in the subject name includes the string of abc.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup] attribute 1 subject-name
dn ctn abc
```

Create a certificate attribute rule, specifying that the FQDN in the issuer name cannot be the string of abc.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 2 issuer-name f
qdn nequ abc
```

Create a certificate attribute rule, specifying that the IP address in the alternative subject name cannot be 10.0.0.1.

```
[Sysname-pki-cert-attribute-group-mygroup] attribute 3 alt-subject-n
ame ip nequ 10.0.0.1
```

ca identifier

Syntax **ca identifier** *name*

undo ca identifier

View PKI domain view

Parameter *name*: Identifier of the trusted CA, a case-insensitive string of 1 to 63 characters

Description Use the **ca identifier** command to specify the trusted CA, and bind the device with the CA *name*.

Use the **undo ca identifier** command to remove the configuration.

By default, no trusted CA is specified for a PKI domain.

Certificate request, retrieval, revocation, and query all depend on the trusted CA.

Example # Specify the trusted CA as new-ca.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ca identifier new-ca
```

certificate request entity

Syntax **certificate request entity** *entity-name*

undo certificate request entity

View PKI domain view

Parameter *entity-name*: Name of the entity for certificate request, a case-insensitive string of 1 to 15 characters.

Description Use the **certificate request entity** command to specify the entity for certificate request.

Use the **undo certificate request entity** command to remove the configuration.

By default, no entity is specified for a PKI domain.

Related command: **pki entity**.

Example # Specify the entity for certificate request as entity1.

```
<SysnameCA> system-view
[SysnameCA] pki domain 1
[SysnameCA-pki-domain-1] certificate request entity entity1
```

certificate request from

Syntax **certificate request from** { **ca** | **ra** }

undo certificate request from

View PKI domain view

Parameter **ca**: Indicates that the entity requests a certificate from a CA.

ra: Indicates that the entity requests a certificate from an RA.

Description Use the **certificate request from** command to specify the authority for certificate request.

Use the **undo certificate request from** command to remove the configuration.

By default, no authority is specified for a PKI domain view.

Example # Specify that the entity requests a certificate from the CA.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request from ca
```

certificate request mode

Syntax **certificate request mode** { **auto** [**key-length** *key-length* | **password** { **cipher** | **simple** } *password*]*| **manual**}

undo certificate request mode

View PKI domain view

Parameter **auto**: Specifies to request a certificate in auto mode.

key-length: Length of the RSA key, in the range 512 to 2048 bits. It is 1024 bits by default.

password: Password used for revoking a certificate, a case-sensitive string of 1 to 31 characters.

cipher: Specifies to display the password in cipher text.

simple: Specifies to display the password in clear text.

manual: Specifies to request a certificate in manual mode.

Description Use the **certificate request mode** command to configure the certificate request mode.

Use the **undo certificate request mode** command to restore the default mode.

By default, manual mode is used.

In auto mode, an entity automatically requests a certificate from an RA or CA when it has no certificate or when the existing certificate is about to expire. In manual mode, all operations associated with certificate request are carried out manually.

Related command: **pki request-certificate domain**.

Example # Specify to request a certificate in auto mode.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request mode auto
```

certificate request polling

Syntax **certificate request polling** { **count** *count* | **interval** *minutes* }

undo certificate request polling { **count** | **interval** }

View PKI domain view

Parameter *count*: Maximum number of attempts to poll the status of the certificate request, in the range 1 to 100.

minutes: Polling interval, in the range 5 to 168 minutes.

Description Use the **certificate request polling** command to specify the certificate request polling interval and maximum number of attempts.

Use the **undo certificate request polling** command to restore the defaults.

By default, the polling is executed once every 20 minutes for up to 50 times.

After an applicant makes a certificate request, the CA may need a long period of time if it verifies the certificate request manually. During this period, the applicant needs to query the status of the request periodically to get the certificate as soon as possible after the certificate is signed.

Related command: **display pki certificate**.

Example # Specify the polling interval as 15 minutes and the maximum number of attempts as 40.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request polling interval 15
[Sysname-pki-domain-1] certificate request polling count 40
```

certificate request url

Syntax **certificate request url** *url-string*

undo certificate request url

View PKI domain view

Parameter *url-string*: URL of the server for certificate request, a case-insensitive string of 1 to 127 characters. It comprises the location of the server and the location of CGI command interface script in the format of *http://server_location/ca_script_location*, where *server_location* is generally expressed in IP address.

Description Use the **certificate request url** command to specify the URL of the RA server that the device makes a certificate request through SCEP.

Use the **undo certificate request url** command to remove the configuration.

By default, no URL is specified for a PKI domain.

Example # Specify the URL of the server for certificate request.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] certificate request url
http://169.254.0.100/certsrv/mscep/mscep.dll
```

common-name

Syntax **common-name** *name*

undo common-name

View PKI entity view

Parameter *name*: Common name of an entity, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description Use the **common-name** command to configure the common name of an entity, which can be, for example, the user name

Use the **undo common-name** command to remove the configuration.

By default, no common name is specified.

Example # Configure the common name of an entity as test.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] common-name pki test
```

country

Syntax **country** *country-code-str*

undo country

View PKI entity view

Parameter *country-code-str*: Country code for the entity, a 2-character case-insensitive string.

Description Use the **country** command to specify the code of the country to which an entity belongs. It is a standard 2-character code, for example, CN for China.

Use the **undo country** command to remove the configuration.

By default, no country code is specified.

Example # Set the country code of an entity to CN.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] country CN
```

crl check

Syntax **crl check** { **disable** | **enable** }

View PKI domain view

Parameter **disable**: Disables CRL checking.

enable: Enables CRL checking.

Description Use the **crl check** command to enable or disable CRL checking.

By default, CRL checking is enabled.

CRLs are files issued by the CA to distribute all certificates have been revoked. Revocation of a certificate may occur before the certificate expires. CRL checking is intended for checking whether a certificate has been revoked. A revoked certificate is no longer trusted.

Example # Disable CRL checking.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl check disable
```

crl update-period

Syntax **crl update-period** *hours*

undo crl update-period

View PKI domain view

Parameter *hours*: CRL update period, in the range 1 to 720 hours.

Description Use the **crl update-period** command to set the CRL update period, that is, the interval at which the PKI entity downloads the latest CRL.

Use the **undo crl update-period** command to restore the default.

By default, the CRL update period depends on the next update field in the CRL file.

The CRL update period is the interval at which a PKI entity with a certificate downloads a CRL from LDAP server.

Example # Set the CRL update period to 20 hours.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl update-period 20
```

crl url

Syntax **crl url** *url-string*

undo crl url

View PKI domain view

Parameter *url-string*: URL of the CRL distribution point, a case-insensitive string of 1 to 127 characters in the format of *ldap: //server_location*, where *server_location* is generally expressed by IP address.

Description Use the **crl url** command to specify the URL of the CRL distribution point.

Use the **undo crl url** command to remove the configuration.

By default, no CRL distribution point URL is specified.

Note that when the URL of the CRL distribution point is not set, you should acquire CA certificate and a local certificate, and then acquire a CRL through SCEP.

Example # Specify the URL of the CRL distribution point.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] crl url ldap://169.254.0 30
```

display pki certificate

Syntax **display pki certificate** { { **ca** | **local** } **domain** *domain-name* | **request-status** }

View Any view

Parameter **ca**: Displays the CA certificate.

local: Displays the local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

request-status: Displays the status of a certificate request.

Description Use the **display pki certificate** command to display the contents of a certificate or the status of certificate request.

Related command: **pki retrieval-certificate**, **pki domain** and **certificate request polling**.

Example # Display the local certificate.

```
<Sysname> display pki certificate local domain 1
Data:
        Version: 3 (0x2)
        Serial Number:
            10B7D4E3 00010000 0086
        Signature Algorithm:  md5WithRSAEncryption
        Issuer:
            emailAddress=myca@aabbcc.net
            C=CN
            ST=Country A
            L=City X
            O=abc
            OU=bjs
            CN=new-ca
        Validity
            Not Before:  Jan 13 08: 57: 21 2004 GMT
            Not After :  Jan 20 09: 07: 21 2005 GMT
        Subject:
            C=CN
            ST=Country B
            L=City Y
            CN=pki test
        Subject Public Key Info:
            Public Key Algorithm:  rsaEncryption
            RSA Public Key:  (512 bit)
                Modulus (512 bit):
                    00D41D1F ...
                Exponent:  65537 (0x10001)
        X509v3 extensions:
            X509v3 Subject Alternative Name:
            DNS: hyf.xxyyzz.net
            X509v3 CRL Distribution Points:
            URI:http://1.1.1.1:447/myca.crl
            ...          ...
    Signature Algorithm:  md5WithRSAEncryption
        A3A5A447 4D08387D ...
```

Table 532 Description on the fields of the display pki certificate command

Field	Description
Version	Version of the certificate
Serial Number	Serial number of the certificate
Signature Algorithm	Signature algorithm
Issuer	Issuer of the certificate
Validity	Validity period of the certificate
Subject	Entity holding the certificate
Subject Public Key Info	Public key information of the entity
X509v3 extensions	Extensions of X509 (version 3) certificate
X509v3 CRL Distribution Points	Distribution points of X509 (version 3) CRL

display pki certificate access-control-policy

Syntax **display pki certificate access-control-policy** { *policy-name* | **all** }

View Any view

Parameter *policy-name*: Name of the certificate attribute-based access control policy, a string of 1 to 16 characters.

all: Displays all certificate attribute-based access control policies.

Description Use the **display pki certificate access-control-policy** command to display information about a specified or all certificate attribute-based access control policies.

Example # Display the information of the certificate attribute-based access control policy named mypolicy.

```
<Sysname> display pki certificate access-control-policy mypolicy
 access-control-policy name: mypolicy
     rule  1 deny    mygroup1
     rule  2 permit  mygroup2
```

Table 533 Description on the fields of the display pki certificate access-control-policy command

Field	Description
access-control-policy	Name of the certificate attribute-based access control policy
rule number	Number of the access control rules

display pki certificate attribute-group

Syntax **display pki certificate attribute-group** { *group-name* | **all** }

View Any view

Parameter *group-name*: Name of a certificate attribute group, a string of 1 to 16 characters.

all: Specifies all certificate attribute groups.

Description Use the **display pki certificate attribute-group** command to display the information of a specified or all certificate attribute groups.

Example # Display the information of certificate attribute group mygroup.

```
<Sysname> display pki certificate attribute-group mygroup
 attribute group name: mygroup
      attribute  1 subject-name     dn    ctn   abc
      attribute  2 issuer-name      fqdn  nctn  apple
```

Table 534 Description on the fields of display pki certificate attribute-group

Field	Description
attribute group name	Name of the certificate attribute group
attribute number	Number of the attribute rules
subject-name	Name of the certificate subject
dn	Domain of the entity
ctn	Indicates the contain operations
abc	Value of attribute 1
issuer-name	Name of the certificate issuer
fqdn	FQDN of the entity
nctn	Indicates the not-contain operations
app	Value of attribute 2

display pki crl domain

Syntax **display pki crl domain** *domain-name*

View Any view

Parameter *domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

Description Use the **display pki crl domain** command to display the locally saved CRLs.

Related command: **pki retrieval-crl domain** and **pki domain**.

Example # Display the locally saved CRLs.

```
<Sysname> display pki crl domain 1
 Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm:  sha1WithRSAEncryption
        Issuer:
            C=CN
            O=abc
            OU=soft
            CN=A Test Root
        Last Update:  Jan  5 08: 44: 19 2004 GMT
        Next Update:  Jan  5 21: 42: 13 2004 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
            keyid:0F71448E E075CAB8 ADDB3A12 0B747387 45D612EC
            Revoked Certificates:
            Serial Number: 05a234448E...
            Revocation Date: Sep  6 12:33:22 2004 GMT
            CRL entry extensions:...
            Serial Number: 05a234448E...
            Revocation Date: Sep  6 12:33:22 2004 GMT
            CRL entry extensions:...
```

Table 535 Description on the fields of the display pki crl domain command

Field	Description
Version	Version of the CRLs
Signature Algorithm	Signature algorithm adopted by the CRLs
Issuer	CA issuing the CRLs
Last Update	Last update time
Next Update	Next update time
CRL extensions	Extensions of CRL
X509v3 Authority Key Identifier	CA issuing the CRLs. The certificate version is X509v3
keyid	ID of the public key
Revoked Certificates	Revoked certificates
Serial Number	Serial number of the revoked certificate
Revocation Date	Revocation date of the certificate

fqdn

Syntax **fqdn** *name-str*

undo fqdn

View PKI entity view

Parameter *name-str*: Fully qualified domain name (FQDN) of an entity, a case-insensitive string of 1 to 127 characters

Description Use the **fqdn** command to configure the FQDN of an entity.

Use the **undo fqdn** command to remove the configuration.

By default, no FQDN is specified for an entity.

An FQDN is the unique identifier of an entity on a network. It consists of a host name and a domain name and can be resolved into an IP address.

Example # Configure the FQDN of an entity as pki.domain-name.com.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] fqdn pki.domain-name.com
```

ip (PKI entity view)

Syntax **ip** *ip-address*

undo ip

View PKI entity view

Parameter *ip-address*: IP address for an entity.

Description Use the **ip** command to configure the IP address of an entity.

Use the **undo ip** command to remove the configuration.

By default, no IP address is specified for an entity.

Example # Configure the IP address of an entity as 11.0.0.1.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] ip 11.0.0.1
```

ldap-server

Syntax **ldap-server ip** *ip-address* [**port** *port-number*] [**version** *version-number*]

undo ldap-server

View PKI domain view

Parameter *ip-address*: IP address of the LDAP server in dotted decimal format.

port-number: Port number of the LDAP server, in the range 1 to 65535. By default, it is 389.

version-number: LDAP version number, either 2 or 3. By default, it is 2.

Description Use the **ldap-server** command to specify an LDAP server for a PKI domain.

Use the **undo ldap-server** command to remove the configuration.

By default, no LDAP server is specified for a PKI domain.

Example # Specify an LDAP server for PKI domain 1.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] ldap-server ip 169.254.0 30
```

locality

Syntax **locality** *locality-name*

undo locality

View PKI entity view

Parameter *locality-name*: Name for the geographical locality, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description Use the **locality** command to configure the geographical locality of an entity, which can be, for example, a city name.

Use the **undo locality** command to remove the configuration.

By default, no geographical locality is specified for an entity.

Example # Configure the locality of an entity as city.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] locality city
```

organization

Syntax **organization** *org-name*

undo organization

View PKI entity view

Parameter *org-name*: Organization name, a case-insensitive string of 1 to 31 characters. No comma can be included

Description Use the **organization** command to configure the name of the organization to which the entity belongs.

Use the **undo organization** command to remove the configuration.

By default, no organization name is specified for an entity.

Example # Configure the name of the organization to which an entity belongs as org-name.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organization org-name
```

organizational-unit

Syntax **organizational-unit** *org-unit-name*

undo organizational-unit

View PKI entity view

Parameter *org-unit-name*: Organization unit name, a case-insensitive string of 1 to 31 characters. No comma can be included. This argument is intended to distinguish different units in an organization.

Description Use the **organizational-unit** command to specify the name of the organization unit to which this entity belongs.

Use the **undo organizational-unit** command to remove the configuration.

By default, no organization unit name is specified for an entity.

Example # Configure the name of the organization unit to which an entity belongs as unit-name.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] organizational-unit unit-name
```

pki certificate access-control-policy

Syntax **pki certificate access-control-policy** *policy-name*

undo pki certificate access-control-policy { *policy-name* | **all** }

View System view

Parameter *policy-name*: Name of the certificate attribute-based access control policy, a case-insensitive string of 1 to 16 characters. It cannot be "a", "al" or "all".

all: Specifies all certificate attribute-based access control policies.

Description Use the **pki certificate access-control-policy** command to create a certificate attribute-based access control policy and enter its view.

Use the **undo pki certificate access-control-policy** command to remove a specified or all certificate attribute-based access control policies.

No access control policy exists by default.

Example # Configure an access control policy named mypolicy and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname-pki-cert-acp-mypolicy]
```

pki certificate attribute-group

Syntax **pki certificate attribute-group** *group-name*

undo pki certificate attribute-group { *group-name* | **all** }

View System view

Parameter *group-name*: Name for the certificate attribute group, a case-insensitive string of 1 to 16 characters. It cannot be "a", "al" or "all".

all: Specifies all certificate attribute groups.

Description Use the **pki certificate attribute-group** command to create a certificate attribute group and enter its view.

Use the **undo pki certificate attribute-group** command to delete one or all certificate attribute groups.

By default, no certificate attribute group exists.

Example # Create a certificate attribute group named mygroup and enter its view.

```
<Sysname> system-view
[Sysname] pki certificate attribute-group mygroup
[Sysname-pki-cert-attribute-group-mygroup]
```

pki delete-certificate

Syntax **pki delete-certificate** { **ca** | **local** } **domain** *domain-name*

View System view

Parameter **ca**: Deletes the locally stored CA certificates.

local: Deletes the locally stored local certificates.

domain-name: Name of the PKI domain whose certificates are to be deleted, a string of 1 to 15 characters.

Description Use the **pki delete-certificate** command to delete locally stored certificates.

Example # Delete the local certificate for PKI domain named cer.

```
<Sysname> system-view
[Sysname] pki delete-certificate local domain cer
```

pki domain

Syntax **pki domain** *domain-name*

undo pki domain *domain-name*

View System view

Parameter *Domain-name*: PKI domain name, a case-insensitive string of 1 to 15 characters.

Description Use the **pki domain** command to create a PKI domain and enter PKI domain view or enter the view of an existing PKI domain.

Use the **undo pki domain** command to remove a PKI domain.

By default, no PKI domain exists.

Example # Create a PKI domain and enter its view.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1]
```

pki entity

Syntax **pki entity** *entity-name*

undo pki entity *entity-name*

View System view

Parameter *entity-name*: Name for the entity, a case-insensitive string of 1 to 15 characters.

Description Use the **pki entity** command to create a PKI entity and enter its view.

Use the **undo pki entity** command to remove a PKI entity.

By default, no entity exists.

You can configure a variety of attributes for an entity in PKI entity view. An entity is intended only for convenience of reference by other commands.

Example # Create a PKI entity named en and enter its view.

```
<Sysname> system-view
[Sysname] pki entity en
[Sysname-pki-entity-en]
```

pki import-certificate

Syntax **pki import-certificate** { **ca** | **local** } **domain** *domain-name* { **der** | **p12** | **pem** } [**filename** *filename*]

View System view

Parameter **ca**: Specifies a CA certificate.

local: Specifies a local certificate.

domain-name: Name of the PKI domain, a string of 1 to 15 characters.

der: Specifies the certificate format of DER.

p12: Specifies the certificate format of P12.

pem: Specifies the certificate format of PEM.

filename *filename*: Name of the certificate file, a case-insensitive string of 1 to 127 characters. It defaults to *domain-name*_ca.cer or *domain-name*_local.cer, the name for the file to be created to save the imported certificate.

Description Use the **pki import-certificate** command to import a CA certificate or local certificate from a file and save it locally.

Related command: **pki domain**.

Example # Import the CA certificate for PKI domain cer in the format of PEM.

```
<Sysname> system-view
[Sysname] pki import-certificate ca domain cer pem
```

pki request-certificate domain

Syntax **pki request-certificate domain** *domain-name* [*password*] [**pkcs10** [**filename** *filename*]]

View System view

Parameter *domain-name*: Name of the PKI domain name, a string of 1 to 15 characters.

password: Password for certificate revocation, a case-sensitive string of 1 to 31 characters.

pkcs10: Displays the BASE64-encoded PKCS#10 certificate request.

filename: Name of the file for saving the PKCS#10 certificate request, a case-insensitive string of 1 to 127 characters.

Description Use the **pki request-certificate domain** command to request a local certificate from a CA through SCEP. If SCEP fails, you can use the **pkcs10** keyword to save the local certificate request in BASE64 format and send it to the CA by an out-of-band means like phone, disk or e-mail.

This operation will not be saved in the configuration file.

Related command: **pki domain**.

Example # Display the PKCS#10 certificate request information.

```
<Sysname> system-view
[Sysname] pki request-certificate domain 1 pkcs10
```

pki retrieval-certificate

Syntax **pki retrieval-certificate** { **ca** | **local** } **domain** *domain-name*

View System view

Parameter **ca**: Downloads a CA certificate.

local: Downloads a local certificate.

domain-name: Name of the PKI domain used for certificate request.

Description Use the **pki retrieval-certificate** command to retrieve a certificate from the server for certificate distribution.

Related command: **pki domain**.

Example # Retrieve the CA certificate from the certificate issuing server.

```
<Sysname> system-view
[Sysname] pki retrieval-certificate ca domain 1
```

pki retrieval-crl domain

Syntax **pki retrieval-crl domain** *domain-name*

View System view

Parameter *domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

Description Use the **pki retrieval-crl** command to retrieve the latest CRLs from the server for CRL distribution.

CRLs are used to validate certificates.

Related command: **pki domain**.

Example # Retrieve CRLs.

```
<Sysname> system-view
[Sysname] pki retrieval-crl domain 1
```

pki validate-certificate

Syntax **pki validate-certificate** { **ca** | **local** } **domain** *domain-name*

View System view

Parameter **ca**: Validates the CA certificate.

local: Validate the local certificate.

domain-name: Name of the PKI domain the certificate to be validated is for, a string of 1 to 15 characters.

Description Use the **pki validate-certificate** command to verify the validity of a certificate.

The focus of certificate validity verification is to check that the certificate is signed by the CA and that the certificate has neither expired nor been revoked.

Related command: **pki domain**.

Example # Verify the validity of the local certificate.

```
<Sysname> system-view
[Sysname] pki validate-certificate domain 1
```

root-certificate fingerprint

Syntax **root-certificate fingerprint** { **md5** | **sha1** } *string*

undo root-certificate fingerprint

View PKI domain view

Parameter **md5**: Uses an MD5 fingerprint.

sha1: Use a SHA1 fingerprint.

string: Fingerprint to be used. An MD5 fingerprint must be a string of 32 characters in hexadecimal. A SHA1 fingerprint must be a string of 40 characters in hexadecimal.

Description Use the **root-certificate fingerprint** command to configure the fingerprint to be used for validating the CA root certificate.

Use the **undo root-certificate fingerprint** command to remove the configuration.

By default, no fingerprint is configured for validating the CA root certificate.

Example # Configure an MD5 fingerprint for validating the CA root certificate.

```
<Sysname> system-view
[Sysname] pki domain 1
[Sysname-pki-domain-1] root-certificate fingerprint md5 12EF53FA355C
D23E12EF53FA355CD23E
```

Configure a SHA1 fingerprint for validating the CA root certificate.

```
[Sysname-pki-domain-1] root-certificate fingerprint sha1 D1526110AAD
7527FB093ED7FC037B0B3CDDDAD93
```

rule (access control policy view)

Syntax **rule** [*id*] { **deny** | **permit** } *group-name*

undo rule { *id* | **all** }

View Access control policy view

Parameter *id*: Number of the certificate attribute-based access control rule, in the range 1 to 16. The default is the smallest unused number in this range.

deny: Indicates that a certificate matching an attribute rule in the specified attribute group is considered invalid and denied.

permit: Indicates that a certificate matching an attribute rule in the specified attribute group is considered valid and permitted.

group-name: Name of the certificate attribute group to be associated with the rule, a case-insensitive string of 1 to 16 characters. It cannot be "a", "al" or "all".

all: Specifies all access control rules.

Description Use the **rule** command to create a certificate attribute access control rule.

Use the **undo rule** command to delete a specified or all access control rules.

By default, no access control rule exists.

Note that a certificate attribute group must exist to be associated with a rule.

Example # Create an access control rule, specifying that a certificate is considered valid it matches an attribute rule in the certificate attribute group mygroup.

```
<Sysname> system-view
[Sysname] pki certificate access-control-policy mypolicy
[Sysname -pki-cert-acp-mypolicy] rule 1 permit mygroup
```

state

Syntax **state** *state-name*

undo state

View PKI entity view

Parameter *state-name*: State or province name, a case-insensitive string of 1 to 31 characters. No comma can be included.

Description Use the **state** command to specify the name of the state or province where an entity resides.

Use the **undo state** command to remove the configuration.

By default, no state or province is specified.

Example # Specify the state where an entity resides.

```
<Sysname> system-view
[Sysname] pki entity 1
[Sysname-pki-entity-1] state Country
```

135 PORTAL CONFIGURATION COMMANDS

display portal acl

Syntax **display portal acl** { **all** | **dynamic** | **static** } **interface** *interface-type interface-number*

View Any view

Parameter **all**: Displays all access control lists (ACLs), including dynamic ACLs and static ACLs.

dynamic: Displays dynamic ACLs, namely, ACLs generated after a user passes portal authentication.

static: Displays static ACLs, namely, ACLs generated by related configurations.

interface *interface-type interface-number*: Displays the ACLs on the specified interface.

Description Use the **display portal acl** command to display the ACLs on the specified interface.

Example # Display all ACLs on Ethernet 1/0.

```
<Sysname> display portal acl all interface ethernet 1/0
Ethernet1/0 portal ACL rule:
 Rule 0
 Inbound interface = Ethernet1/0
 Type              = static
 Action            = permit
 Source:
    IP        = 0.0.0.0
    Mask      = 0.0.0.0
    MAC       = 0000-0000-0000
    Interface = any
    VLAN      = 0
 Destination:
    IP        = 192.168.0.111
    Mask      = 255.255.255.255

 Rule 1
 Inbound interface = Ethernet1/0
 Type              = dynamic
 Action            = permit
 Source:
    IP        = 2.2.2.2
    Mask      = 255.255.255.255
```

```
    MAC        = 000d-88f8-0eab
    Interface  = GigabitEthernet5/0
    VLAN       = 0
 Destination:
    IP         = 0.0.0.0
    Mask       = 0.0.0.0
```

Table 536 Description on the fields of the display portal acl command

Field	Description
Rule	Sequence number of the generated ACL, which is numbered from 0 in ascending order
Inbound interface	Interface to which a portal ACL is bound
Type	Type of a portal ACL
Action	Match action in a portal ACL
Source	Source information in a portal ACL
IP	Source IP address in a portal ACL
Mask	Subnet mask of the source IP address in a portal ACL
MAC	Source MAC address in a portal ACL
Interface	Source interface in a portal ACL
VLAN	Source VLAN in a portal ACL
Destination	Destination information in a portal ACL
IP	Destination IP address in a portal ACL
Mask	Subnet mask of the destination IP address in a portal ACL

display portal connection statistics

Syntax **display portal connection statistics** { **all** | **interface** *interface-type interface-number* }

View Any view

Parameter **all**: Displays portal connection statistics on all interfaces.

interface *interface-type interface-number*: Displays the portal connection statistics on the specified interface.

Description Use the **display portal connection statistics** command to display the portal connection statistics on the specified interface or all interfaces.

Example # Display the portal connection statistics on Ethernet 1/0.

```
<Sysname> display portal connection statistics interface ethernet 1/0
 ---------------Interface: Ethernet1/0-----------------------
 User state statistics:
 State-Name                User-Num
 VOID                       0
 DISCOVERED                 0
 WAIT_AUTHEN_ACK           0
 WAIT_AUTHOR_ACK           0
 WAIT_LOGIN_ACK            0
 WAIT_ACL_ACK               0
 WAIT_NEW_IP                0
```

```
WAIT_USERIPCHANGE_ACK   0
ONLINE                    1
WAIT_LOGOUT_ACK          0
WAIT_LEAVING_ACK         0

Message statistics:
Msg-Name                  Total          Err            Discard
MSG_AUTHEN_ACK           3              0              0
MSG_AUTHOR_ACK           3              0              0
MSG_LOGIN_ACK            3              0              0
MSG_LOGOUT_ACK           2              0              0
MSG_LEAVING_ACK          0              0              0
MSG_CUT_REQ               0              0              0
MSG_AUTH_REQ              3              0              0
MSG_LOGIN_REQ             3              0              0
MSG_LOGOUT_REQ            2              0              0
MSG_LEAVING_REQ           0              0              0
MSG_ARPPKT                 0              0              0
MSG_TMR_REQAUTH           1              0              0
MSG_TMR_AUTHEN            0              0              0
MSG_TMR_AUTHOR            0              0              0
MSG_TMR_LOGIN             0              0              0
MSG_TMR_LOGOUT            0              0              0
MSG_TMR_LEAVING           0              0              0
MSG_TMR_NEWIP             0              0              0
MSG_TMR_USERIPCHANGE     0              0              0
MSG_PORT_REMOVE           0              0              0
MSG_VLAN_REMOVE           0              0              0
MSG_IF_REMOVE             6              0              0
MSG_L3IF_SHUT             0              0              0
MSG_IP_REMOVE             0              0              0
MSG_ALL_REMOVE            1              0              0
MSG_IFIPADDR_CHANGE      0              0              0
MSG_SOCKET_CHANGE        8              0              0
```

Table 537 Description on the fields of the display portal connection statistics command

Field	Description
User state statistics	Statistics of portal users
State-Name	Name of a user state
User-Num	Number of users
VOID	Number of users in void state
DISCOVERED	Number of users in discovered state
WAIT_AUTHEN_ACK	Number of users in wait_authen_ack state
WAIT_AUTHOR_ACK	Number of users in wait_author_ack state
WAIT_LOGIN_ACK	Number of users in wait_login_ack state
WAIT_ACL_ACK	Number of users in wait_acl_ack state
WAIT_NEW_IP	Number of users in wait_new_ip state
WAIT_USERIPCHANGE_ACK	Number of users wait_useripchange_ack state
ONLINE	Number of users in online state
WAIT_LOGOUT_ACK	Number of users in wait_logout_ack state
WAIT_LEAVING_ACK	Number of users in wait_leaving_ack state
Message statistics	Statistics of messages
Msg-Name	Name of a message
Total	Total number of messages
Err	Number of error messages
Discard	Number of discarded messages

Table 537 Description on the fields of the display portal connection statistics command

Field	Description
MSG_AUTHEN_ACK	Authentication acknowledgment message
MSG_AUTHOR_ACK	Authorization acknowledgment message
MSG_LOGIN_ACK	Accounting acknowledgment message
MSG_LOGOUT_ACK	Accounting-stop acknowledgment message
MSG_LEAVING_ACK	Leaving acknowledgment message
MSG_CUT_REQ	Cut request message
MSG_AUTH_REQ	Authentication request message
MSG_LOGIN_REQ	Accounting request message
MSG_LOGOUT_REQ	Accounting-stop request message
MSG_LEAVING_REQ	Leaving request message
MSG_ARPPKT	ARP message
MSG_TMR_REQAUTH	Authentication request timeout message
MSG_TMR_AUTHEN	Authentication timeout message
MSG_TMR_AUTHOR	Authorization timeout message
MSG_TMR_LOGIN	Accounting-start timeout message
MSG_TMR_LOGOUT	Accounting-stop timeout message
MSG_TMR_LEAVING	Leaving timeout message
MSG_TMR_NEWIP	Public IP update timeout message
MSG_TMR_USERIPCHANGE	User IP change timeout message
MSG_PORT_REMOVE	Layer 2 interface user removed message
MSG_VLAN_REMOVE	VLAN user removed message
MSG_IF_REMOVE	Layer 3 interface user removed message
MSG_L3IF_SHUT	Layer 3 interface shutdown message
MSG_IP_REMOVE	IP removed message
MSG_ALL_REMOVE	All users removed message
MSG_IFIPADDR_CHANGE	Interface IP address change message
MSG_SOCKET_CHANGE	Socket change message

display portal free-rule

Syntax **display portal free-rule** [*rule-number*]

View Any view

Parameter *rule-number*: Number of an authentication-free rule. The value range varies with devices.

Description Use the **display portal free-rule** command to display the information of a specified portal-authentication-free rule or all authentication-free rules.

Note that the information of all authentication-free rules will be displayed if the *rule-number* argument is not specified.

Related command: **portal free-rule**.

Example # Display the information of authentication-free rule 1.

```
<Sysname> display portal free-rule 1
 Rule-Number  1:
 Source:
   IP        = 2.2.2.0
   Mask      = 255.255.255.0
   MAC       = 0000-0000-0000
   Interface = any
   Vlan      = 0
 Destination:
   IP        = 0.0.0.0
   Mask      = 0.0.0.0
```

Table 538 Description on the fields of the display portal free-rule command

Field	Description
Rule-Number	Number of an authentication-free rule
Source	Source information in an authentication-free rule
IP	Source IP address in an authentication-free rule
Mask	Subnet mask of the source IP address in an authentication-free rule
MAC	Source MAC address in an authentication-free rule
Interface	Source interface in an authentication-free rule
Vlan	Source VLAN in an authentication-free rule
Destination	Destination information in an authentication-free rule
IP	Destination IP address in an authentication-free rule
Mask	Subnet mask of the destination IP address in an authentication-free rule

display portal interface

Syntax **display portal interface** *interface-type interface-number*

View Any view

Parameter **interface** *interface-type interface-number*: Specifies an interface by interface type and interface number.

Description Use the **display portal interface** command to display the portal configuration on the specified interface.

Example # Display the portal configuration on Ethernet 1/0.

```
<Sysname> display portal interface ethernet 1/0
 Interface portal configuration:
 Ethernet1/0: Portal running
 Portal server: servername
 Authentication type: Direct
 Service type: Normal
 Authentication network:
 address = 0.0.0.0  mask = 0.0.0.0
```

Table 539 Description on the fields of the display portal interface command

Field	Description
Interface portal configuration	Portal configuration on an interface
Ethernet 1/0	Portal state on an interface
Portal server	Portal server applied to an interface
Authentication type	Authentication mode enabled on an interface
Service type	Type of service
Authentication network	Information of an portal authentication subnet
address	IP address of the portal authentication subnet
mask	Subnet mask of the IP address of the portal authentication subnet

display portal server

Syntax **display portal server** [*server-name*]

View Any view

Parameter *server-name*: Name of a portal server, a case-sensitive string of 1 to 32 characters.

Description Use the **display portal server** command to display information about the specified portal server or all portal servers.

Note that the information of all portal servers will be displayed if the *server-name* argument is not specified.

Related command: **portal server**.

Example # Display the information of the portal server named **aaa**.

```
<Sysname> display portal server aaa
 Portal server:
  1)aaa:
    IP   = 192.168.0.111
    Key  = portal
    Port = 50100
    URL  = http://192.168.0.111/portal
```

Table 540 Description on the fields of the display portal server command

Field	Description
1)	Number of the portal server
aaa	Name of the portal server
IP	IP address of the portal server
Key	Key for portal authentication
Port	Listening port on the portal server
URL	Address the packets are to be redirected to

display portal server statistics

Syntax **display portal server statistics** { **all** | **interface** *interface-type interface-number* }

View Any view

Parameter **all**: Displays portal server statistics on all interfaces.

interface *interface-type interface-number*: Displays portal server statistics on the specified interface.

Description Use the **display portal server statistics** command to display portal server statistics on the specified interface or all interfaces, including the information of the packets from and to the portal server.

Note that when the **all** keyword is specified, the device will display the portal server statistics on each interface in turn, even if there is only one portal server.

Example # Display the portal server statistics on Ethernet 1/0.

```
<Sysname> display portal server statistics interface ethernet 1/0
 ---------------Interface: Ethernet1/0----------------------
 Server name:  st
 Invalid packets: 0
 Pkt-Name                          Total   Discard  Checkerr
 REQ_CHALLENGE                       3         0         0
 ACK_CHALLENGE                       3         0         0
 REQ_AUTH                             3         0         0
 ACK_AUTH                             3         0         0
 REQ_LOGOUT                           1         0         0
 ACK_LOGOUT                           1         0         0
 AFF_ACK_AUTH                         3         0         0
 NTF_LOGOUT                           1         0         0
 REQ_INFO                               6         0         0
 ACK_INFO                               6         0         0
 NTF_USERDISCOVER                    0         0         0
 NTF_USERIPCHANGE                    0         0         0
 AFF_NTF_USERIPCHANGE                0         0         0
 ACK_NTF_LOGOUT                       1         0         0
```

Table 541 Description on the fields of the display portal server statistics command

Field	Description
Interface	Interface where the portal server resides on
Server name	Name of the portal server
Invalid packets	Number of invalid packets
Pkt-Name	Packet name
Total	Total number of packets
Discard	Number of discarded packets
Checkerr	Number of error packets
REQ_CHALLENGE	Challenge request message the portal server sends to the access device

Table 541 Description on the fields of the display portal server statistics command

Field	Description
ACK_CHALLENGE	Challenge acknowledgment message the access device sends to the portal server
REQ_AUTH	Authentication request message the portal server sends to the access device
ACK_AUTH	Authentication acknowledgment message the access device sends to the portal server
REQ_LOGOUT	Logout request message the portal server sends to the access device
ACK_LOGOUT	Logout acknowledgment message the access device sends to the portal server
AFF_ACK_AUTH	Affirmation message the portal server sends to the access device after receiving an authentication success message
NTF_LOGOUT	Forced logout notification message the access device sends to the portal server
REQ_INFO	Information request message
ACK_INFO	Information acknowledgment message
NTF_USERDISCOVER	User discovery notification message the portal server sends to the access device
NTF_USERIPCHANGE	User IP change notification message the access device sends to the portal server
AFF_NTF_USERIPCHANGE	User IP change success notification message the portal server sends to the access device
ACK_NTF_LOGOUT	Forced logout acknowledgment message from the portal server

display portal tcp-cheat statistics

Syntax **display portal tcp-cheat statistics**

View Any view

Parameter None

Description Use the **display portal tcp-cheat statistics** command to display TCP spoofing statistics.

Example # Display all TCP spoofing statistics.

```
<Sysname> display portal tcp-cheat statistics
 TCP Cheat Statistic:
 Total Opens: 0
 Reset Connections: 0
 Current Opens: 0
 Packets Received: 0
 Packets Sent: 0
 Packets Retransmitted: 0
 Packets Dropped: 0
 HTTP Packets Sent: 0
```

```
Connection State:
         SYN_RECVD: 0
         ESTABLISHED: 0
         CLOSE_WAIT: 0
         LAST_ACK: 0
         FIN_WAIT_1: 0
         FIN_WAIT_2: 0
         CLOSING: 0
```

Table 542 Description on fields of the display portal tcp-cheat statistics command

Field	Description
TCP Cheat Statistic	TCP spoofing statistics
Total Opens	Total number of opened connections
Resets Connections	Number of the connections reset through RST packets
Current Opens	Number of active connections
Packets Received	Number of received packets
Packets Sent	Number of sent packets
Packets Retransmitted	Number of retransmitted packets
Packets Dropped	Number of dropped packets
HTTP Packets Sent	Number of sent HTTP packets
Connection State	State of a connection
ESTABLISHED	Number of connections in ESTABLISHED state
CLOSE_WAIT	Number of connections in CLOSE_WAIT state
LAST_ACK	Number of connections in LAST-ACK state
FIN_WAIT_1	Number of connections in FIN_WAIT_1 state
FIN_WAIT_2	Number of connections in FIN_WAIT_2 state
CLOSING	Number of connections in CLOSING state

display portal user

Syntax **display portal user** { **all** | **interface** *interface-type interface-number* }

View Any view

Parameter **all**: Displays user information on all interfaces enabling portal.

interface *interface-type interface-number*: Displays user information on the specified interface enabling portal.

Description Use the **display portal user** command to display user information on the specified interface or all interfaces enabling portal.

Example # Display user information on all interfaces enabling portal.

```
<Sysname> display portal user all
 Index:2
 State:ONLINE
 SubState:INVALID
 MAC               IP                Vlan   Interface
 --------------------------------------------------------------------------
```

```
000d-88f8-0eab   2.2.2.2           0       Ethernet1/0
Total 1 user(s) matched, 1 listed.
```

Table 543 Description on the fields of the display portal user command

Field	Description
Index	Index of a portal user
State	Current state of a portal user
SubState	Current sub-state of a portal user
MAC	MAC address of a portal user
IP	IP address of a portal user
Vlan	VLAN where a portal user is
Interface	Interface to which a portal user is attached
Total 1 user(s) matched, 1 listed	Counts of portal users

portal auth-network

Syntax **portal auth-network** *network-address* { *mask-length* | *mask* }

undo portal auth-network { *network-address* | **all** }

View Interface view

Parameter *network-address*: Authentication subnet address.

mask-length: Length of the subnet mask, in the range of 0 to 32.

mask: Subnet mask, in dotted decimal notation.

all: Specifies all authentication subnets.

Description Use the **portal auth-network** command to configure a portal authentication subnet.

Use the **undo portal auth-network** command to remove the configuration.

Note that this command is applicable to only Layer 3 authentication. The portal authentication subnet for direct authentication is any source IP address, and the portal authentication subnet for re-DHCP authentication is the one determined by the private IP address of the interface.

By default, the portal authentication subnet is 0.0.0.0/0, meaning to authenticate users in all subnets.

Example # Set the portal authentication subnet to 10.10.10.0/24.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] portal auth-network 10.10.10.0 24
```

portal delete-user

Syntax **portal delete-user** { *ip-address* | **all** | **interface** *interface-type interface-number* }

View System view

Parameter *ip-address*: IP address of a user.

all: Forces all users to log out.

interface *interface-type interface-number*: Forces all users on the specified interface to log out.

Description Use the **portal delete-user** command to force the users attached to the access device to log out.

Related command: **display portal user**.

Example # Force the user whose host IP address is 1.1.1.1 to log out.

```
<Sysname> system-view
[Sysname] portal delete-user 1.1.1.1
```

portal free-rule

Syntax **portal free-rule** *rule-number* { **destination** { **any** | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } } | **source** { **any** | [**interface** *interface-type interface-number* | **ip** { *ip-address* **mask** { *mask-length* | *netmask* } | **any** } | **mac** *mac-address*] * } } *

undo portal free-rule { *rule-number* | **all** }

View System view

Parameter *rule-number*: Number of an authentication-free rule. The value range varies with devices.

any: Specifies no limitation on the keyword which comes before the **any** keyword.

ip *ip-address*: Specifies an IP address in an authentication-free rule.

mask { *mask-length* | *netmask* }: Specifies the mask of the IP address, which can be in dotted decimal notation or an integer in the range 0 to 32.

interface *interface-type interface-number*: Specifies a source interface in an authentication-free rule. The support for this option varies with devices.

mac *mac-address*: Specifies a source MAC address (in the H-H-H format) in an authentication-free rule. The support for this option varies with devices.

all: Specifies all authentication-free rules.

Description Use the **portal free-rule** command to configure a portal authentication-free rule, namely, to specify a source filtering condition or destination filtering condition.

Use the **undo portal free-rule** command to remove the authentication-free rule.

If you specify both the source IP and source MAC address information in a portal-free rule, the IP address must be a host address with a mask of 32 bits; otherwise, the specified MAC address will be neglected.

Related command: **display portal free-rule**.

Example # Configure a portal authentication-free rule where the packets whose source IP address is 10.10.10.1/24, source interface is Ethernet 1/0, and destination IP address is any address will not trigger a portal authentication.

```
<Sysname> system-view
[Sysname] portal free-rule 15 source ip 10.10.10.1 mask 24 interface
 ethernet 1/0 destination ip any
```

portal resource-name

Syntax **portal resource-name** *resource-name*

undo portal resource-name

View System view

Parameter *resource-name*: Name of the resource to be protected, a case-sensitive string of 1 to 32 characters.

Description Use the **portal resource-name** command to configure a name for the resource to be protected.

Use the **undo portal resource-name** command to remove the configuration.

By default, the name of the resource to be protected is not specified.

This command only applies to the devices with portal+ enabled.

Example # Configure the name of the resource to be protected as portal-info-center.

```
<Sysname> system-view
[Sysname] portal resource-name portal-info-center
```

portal server

Syntax **portal server** *server-name* **ip** *ip-address* [**key** *key-string* | **port** *port-id* | **url** *url-string*] *

undo portal server *server-name* [**key** | **port** | **url**]

View System view

Parameter *server-name*: Name of the portal server, a case-sensitive string of 1 to 32 characters.

ip-address: IP address of the portal server.

key-string: Shared key required for communication with the portal server, a case-sensitive string of 1 to 16 characters.

port-id: Destination port ID used when the device sends a message to the portal server on its own, in the range 1 to 65534. The default is 50100.

url-string: Uniform resource locator (URL) to which HTTP packets are to be redirected, in the *http://ip-address* format. The default of *ip-address* is the IP address of the portal server.

Description Use the **portal server** command to configure a portal server.

Use the **undo portal server** command to delete the specified portal server or restore the default.

By default, no portal server is configured.

Note that if the specified portal server exists but there is no user on the interface, the specified portal server will be deleted if no parameter is specified when the **undo portal server** command is executed. Otherwise, the **port** and **url** parameters, if specified, will be restored to the default values.

Related command: **display portal server**.

CAUTION:

- *The parameters of a **portal server** are modifiable. If the portal feature is enabled on an interface, the **portal server** applied to the interface cannot be deleted. If there are users on this interface, the parameters of the **portal server** cannot be modified.*
- *You must disable portal authentication on the interface before deleting the **portal server** applied to an interface in system view.*

Example # Configure portal server pts, setting the IP address to 192.168.0.111, the key to portal, and the redirection URL to http://192.168.0.111/portal.

```
<Sysname> system-view
[Sysname] portal server pts ip 192.168.0.111 key portal url http://1
92.168.0.111/portal
```

portal server method

Syntax **portal server** *server-name* **method** { **direct** | **layer3** | **redhcp** } [**service-type** { **normal** | **plus** }]

undo portal

View Interface view

Parameter *server-name*: Name of the portal server, a case-sensitive string of 1 to 32 characters.

Method: Specifies an authentication method.

- **direct**: Direct authentication.
- **layer3**: Layer 3 authentication
- **redhcp**: Re-DHCP authentication.

service-type: Type of service. The default service type is normal.

- **Normal**: Normal portal authentication.
- **Plus**: Extended portal authentication.

Description Use the **portal server** command to enable portal authentication on the interface, and specify the portal server to be referenced, authentication mode and service type.

Use the **undo portal** command to disable portal authentication on the interface.

By default, portal authentication is disabled.

Note that the specified portal server must exist.

Related command: **display portal server**.

Example # Enable portal authentication on interface Ethernet 1/0, specifying the portal server as pts, setting the authentication mode to **direct** and the service type to **normal**.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] portal server pts method direct service-type normal
```

reset portal connection statistics

Syntax **reset portal connection statistics** { **all** | **interface** *interface-type interface-number* }

View User view

Parameter **all**: Clears portal connection statistics on all interfaces.

interface *interface-type interface-number*: Clears the portal connection statistics on the specified interface.

Description Use the **reset portal connection statistics** command to clear the portal connection statistics on the specified interface or all interfaces.

Example # Clear the portal connection statistics on Ethernet 1/0.

```
<Sysname> reset portal connection statistics interface ethernet 1/0
```

reset portal server statistics

Syntax **reset portal server statistics** { **all** | **interface** *interface-type interface-number* }

View User view

Parameter **all**: Clears the portal server statistics on all interfaces.

interface *interface-type interface-number*: Clears the portal server statistics on the specified interface.

Description Use the **reset portal server statistics** command to clear the portal server statistics on the specified interface or all interfaces.

Example # Clear the portal server statistics on Ethernet 1/0.

```
<Sysname> reset portal server statistics interface ethernet 1/0
```

reset portal tcp-cheat statistics

Syntax **reset portal tcp-cheat statistics**

View User view

Parameter None

Description Use the **reset portal tcp-cheat statistics** command to clear TCP spoofing statistics.

Example # Clear TCP spoofing statistics.

```
<Sysname> reset portal tcp-cheat statistics
```

136 RSH CONFIGURATION COMMANDS

rsh

Syntax **rsh** *host* [**user** *username*] **command** *remote-command*

View User view

Parameter *host*: IP address or host name of the remote host, a string of 1 to 20 characters.

user *username*: Specifies the username for remote login, which is a string of 1 to 20 characters. If you specify no username, the system name of the device, which can be set by using the **sysname** command, applies.

remote-command: Command to be executed remotely. The commands available depend on the operating system running on the RSH server.

Description Use the **rsh** command to execute an operating system (OS) command of a remote host.

You can operate on the RSH client to remotely execute the OS commands of the RSH server and query/access information as well.

Example # Display information about the directories and files on remote server 169.254.1.100, which is running Windows 2000.

```
<Sysname> rsh 169.254.1.100 com dir
Trying 169.254.1.100 ...
Press CTRL+K to abort
 Volume in drive C is SYSTEM
 Volume Serial Number is 2A0F-18DF

 Directory of C:WRSHDNT

2004-07-13  09:10       <DIR>          .
2004-07-13  09:10       <DIR>          ..
2001-05-10  09:04               162,304 UNWISE.EXE
2001-12-05  15:36                45,056 wrshdcfg.exe
1996-08-05  15:39                48,128 ctrlrshd.exe
1998-10-13  16:31                31,744 forewin.exe
2004-01-02  23:05                40,625 history.txt
2003-02-26  17:04                 6,822 order.txt
1997-08-26  16:05                23,552 whoami.exe
2001-12-07  17:28               122,880 wrshdctl.exe
2003-06-21  10:51               192,512 wrshdnt.cpl
2001-12-09  16:41                38,991 wrshdnt.hlp
```

```
2001-12-09  16:26                1,740 wrshdnt.cnt
2003-06-22  11:14              452,230 wrshdnt.htm
2003-06-23  18:18                4,803 wrshdnt_header.htm
2003-06-23  18:18                  178 wrshdnt_filelist.xml
2003-06-22  11:13              156,472 wrshdnt.pdf
2001-09-02  15:41               49,152 wrshdrdr.exe
2003-06-21  10:32               69,632 wrshdrun.exe
2004-01-02  15:54              196,608 wrshdsp.exe
2004-01-02  15:54              102,400 wrshdnt.exe
2001-07-30  18:05                  766 wrshdnt.ico
2004-07-13  09:10                3,253 INSTALL.LOG
              21 files      1,749,848 bytes
               2 directories  2,817,417,216 bytes free
```

Set the system time of remote server 169.254.1.100, which is running Windows 2000.

```
<Sysname> rsh 169.254.1.100 command time
Trying 169.254.1.100 ...
Press CTRL+K to abort
The current time is:  6:56:42.57
Enter the new time: 12:00
12:00
```

137 COMMON CONFIGURATION COMMANDS

display time-range

Syntax **display time-range** { *time-name* | **all** }

View Any view

Parameter *time-name*: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

all: All existing time ranges.

Description Use the **display time-range** command to display the configuration and state of a specified or all time ranges.

A time range is active if the system time falls into its range, and if otherwise, inactive.

Example # Display the configuration and state of time range trname.

```
[Sysname] display time-range trname
Current time is 10:45:15 4/14/2005 Thursday
Time-range : trname ( Inactive )
from 08:00 12/1/2005 to 23:59 12/31/2100
```

Table 544 Description on the fields of the display time-range command

Field	Description
Current time	Current system time
Time-range	The configuration and state of time range, such as time range name, its activated state, and start time and ending time.

time-range

Syntax **time-range** *time-name* { *start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* }

undo time-range *time-name* [*start-time* **to** *end-time days* [**from** *time1 date1*] [**to** *time2 date2*] | **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2*]

View System view

Parameter

time-name: Time range name comprising 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

start-time: Start time of a periodic time range, in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59.

end-time: End time of the periodic time range, in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 24:00. The end time must be greater than the start time.

days: Indicates on which day or days of the week the periodic time range is valid. You may specify multiple values, in words or in digits, separated by spaces, for this argument, but make sure that they do not overlap. These values can take one of the following forms:

- A digit in the range 0 to 6, respectively for Sunday, Monday, Tuesday, Wednesday, Thursday, Friday, and Saturday.
- Week in words, that is, **Mon**, **Tue**, **Wed**, **Thu**, **Fri**, **Sat**, or **Sun**.
- **working-day** for Monday through Friday.
- **off-day** for Saturday and Sunday.
- **daily** for seven days of a week.

from *time1 date1*: Indicates the start time and date of an absolute time range. The *time1* argument specifies the time of the day in *hh***:***mm* format as 24-hour time, where *hh* is hours and *mm* is minutes. Its value ranges from 00:00 to 23:59. The *date1* argument specifies a date in *MM***/***DD***/***YYYY* or *YYYY***/***MM***/***DD* format, where *MM* is the month of the year in the range 1 to 12, DD is the day of the month in the range 1 to 31, and YYYY is the year in the usual Gregorian calendar in the range 1970 to 2100. If not specified, the start time is the earliest time available from the system, namely, 01/01/1970 00:00:00 AM.

to *time2 date2*: Indicates the end time and date of the absolute time range. The format of the *time2* argument is the same as that of the *time1* argument, but its value ranges from 00:00 to 24:00. The end time must be greater than the start time. If not specified, the end time is the maximum time available from the system, namely, 12/31/2100 24:00:00 PM. The format and value range of the *date2* argument are the same as those of the *date1* argument.

Description

Use the **time-range** command to create a time range.

Use the **undo time-range** command to remove a time range.

You may create a maximum of 256 time ranges.

A time range can be one of the following:

- Periodic time range created using the **time-range** *time-name start-time* **to** *end-time days* command. A time range thus created recurs periodically on the day or days of the week.
- Absolute time range created using the **time-range** *time-name* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. Unlike a periodic time range, a time range thus created does not recur. For example, to create an

absolute time range that is active between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test from 00:00 01/01/2004 to 23:59 12/31/2004** command.

- Compound time range created using the **time-range** *time-name start-time* **to** *end-time days* { **from** *time1 date1* [**to** *time2 date2*] | **to** *time2 date2* } command. A time range thus created recurs on the day or days of the week only within the specified period. For example, to create a time range that is active from 12:00 to 14:00 on Wednesdays between January 1, 2004 00:00 and December 31, 2004 23:59, you may use the **time-range test 12:00 to 14:00 wednesday from 00:00 01/01/2004 to 23:59 12/31/2004** command.

You may create individual time ranges identified with the same name. They are regarded as one time range whose active period is the result of ORing periodic ones, ORing absolute ones, and ANDing periodic and absolute ones.

Example # Create an absolute time range named test, setting it to become active from 00:00 on January 1, 2003.

```
<Sysname> system-view
[Sysname] time-range test from 0:0 2003/1/1
```

Create a compound time range named test, setting it to be active between 8:00 to 18:00 during working days.

```
<Sysname> system-view
[Sysname] time-range test 8:00 to 18:00 working-day
```

Create a periodic time range named test, setting it to be active between 14:00 and 18:00 on Saturday and Sunday.

```
<Sysname> system-view
[Sysname] time-range test 14:00 to 18:00 off-day
```

138 IPv4 ACL Configuration Commands

acl

Syntax **acl number** *acl-number* [**name** *acl-name*] [**match-order** { **auto** | **config** }]

undo acl { **all | name** *acl-name* | **number** *acl-number* }

View System view

Parameter *acl-number*: IPv4 ACL number in the range 2000 to 5999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

The MSR 20 Series Routers do not support the last range, that 5000 to 5999.

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

match-order: Sets the order in which ACL rules are matched. This keyword is not available for user-defined IPv4 ACLs.

- **auto**: Performs depth-first match.
- **config**: Performs matching against rules in the order in which they are configured.

all: All IPv4 ACLs.

Description Use the **acl** command to enter IPv4 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl** command to remove a specified or all IPv4 ACLs.

By default, the match order is **config**.

Note that:

- You can specify a name for an IPv4 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove the name of the ACL.
- The name of an IPv4 ACL must be unique among IPv4 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- The match order for user-defined ACLs can only be **config**.
- You can also use this command to modify the match order of an existing IPv4 ACL but only when it is empty.

Example # Create IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Create IPv4 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl number 2002 name flow
[Sysname-acl-basic-2002-flow]
```

Enter the view of an IPv4 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000]
```

Enter the view of an IPv4 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl number 2002
[Sysname-acl-basic-2002-flow]
```

Delete the IPv4 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl number 2000
```

Delete the IPv4 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl name flow
```

acl copy

Syntax **acl copy** { *source-acl-number* | **name** *source-acl-name* } **to** { *dest-acl-number* | **name** *dest-acl-name* }

View **System view**

Parameter *source-acl-number*: Number of an existing IPv4 ACL, which must be in the following ranges (the available ACL number ranges varies by device):

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

source-acl-name: Name of an existing IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

dest-acl-number: Number of a non-existent IPv4 ACL, which must be in the following ranges (the available ACL number ranges varies by device):

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

dest-acl-name: Name for the new IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a sequence number which is the smallest one among the available ones in the ACL range for the ACL type.

Description Use the **acl copy** command to copy an existent IPv4 ACL (namely, the source IPv4 ACL) to generate a new one (namely, the destination IPv4 ACL). The new ACL is of the same type and has the same match order, match rules, rule numbering step and descriptions.

Note that:

- The source IPv4 ACL and the destination IPv4 ACL must be of the same type.
- The generated ACL does not take the name of the source IPv4 ACL.

Example # Copy ACL 2008 to generate ACL 2009.

```
<Sysname> system-view
[Sysname] acl copy 2008 to 2009
```

acl name

Syntax **acl name** *acl-name*

View System view

Parameter *acl-name*: Name of the IPv4 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description Use the **acl name** command to enter the view of an existing IPv4 ACL by specifying its name.

Example # Enter the view of the IPv4 ACL named flow.

```
<Sysname> system-view
[Sysname] acl name flow
[Sysname-acl-basic-2002-flow]
```

description (for IPv4)

Syntax **description** *text*

undo description

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view, user-defined ACL view

Parameter *text*: ACL description, a case-sensitive string of 1 to 127 characters.

Description Use the **description** command to create an IPv4 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the ACL description.

By default, an IPv4 ACL has no description configured.

Example # Create a description for IPv4 ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] description This acl is used in eth 0
```

Define the description of IPv4 ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] description This acl is used in eth 0
```

Define the description of ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] description This acl is used in eth 0
```

Define the description of ACL 5000.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] description This acl is used in eth 0
```

display acl

Syntax **display acl** { *acl-number* | **all** | **name** *acl-name* }

View Any view

Parameter *acl-number*: IPv4 ACL number in the range 2000 to 5999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs
- 5000 to 5999 for user-defined ACLs

all: All IPv4 ACLs.

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

The MSR 20 Series Routers do not support the last range, that 5000 to 5999.

Description Use the **display acl** command to display information about the specified or all IPv4 ACLs.

This command displays ACL rules in the order in which the system compares a packet against them.

Example # Display information about IPv4 ACL 2001.

```
<Sysname> display acl 2001
Basic acl  2001, named flow, 1 rule,
Acl's step is 5
 rule 5 permit source 1.1.1.1 0 (5 times matched)
 rule 5 comment This rule is used in eth 1
```

Table 545 Description on the fields of the display acl command

Field	Description
Basic acl 2001	The displayed information is about the basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
Acl's step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. This field appears as long as one match is found.

Table 545 Description on the fields of the display acl command

Field	Description
rule 5 comment This rule is used in eth 1	The description of ACL rule 5 is "This rule is used in eth 1."

reset acl counter

Syntax **reset acl counter** { *acl-number* | **all** | **name** *acl-name* }

View User view

Parameter *acl-number*: IPv4 ACL number in the range 2000 to 4999, where:

- 2000 to 2999 for basic IPv4 ACLs
- 3000 to 3999 for advanced IPv4 ACLs
- 4000 to 4999 for Ethernet frame header ACLs

all: All IPv4 ACLs except for user-defined ACLs.

name *acl-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description Use the **reset acl counter** command to clear statistics about specified or all IPv4 ACLs except for user-defined ACLs.

Example # Clear statistics about IPv4 ACL 2001.

```
<Sysname> reset acl counter 2001
```

Clear statistics about IPv4 ACL flow.

```
<Sysname> reset acl counter name flow
```

rule (in basic IPv4 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *sour-addr sour-wildcard* | **any** } | **time-range** *time-name* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range** | **vpn-instance**] *

View Basic IPv4 ACL view

Parameter *rule-id*: Basic IPv4 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Indicates that the rule applies only to non-first fragments. Without this keyword, the rule applies to both fragments and non-fragments

logging: Specifies to log matched packets. The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.

source { *sour-addr sour-wildcard* | **any** }: Specifies a source address. The *sour-addr sour-wildcard* argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.

time-range *time-name:* Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

vpn-instance *vpn-instance-name:* Specifies a VPN instance. The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.

Description

Use the **rule** command to create a basic IPv4 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove a basic IPv4 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Example

Create a rule to deny packets with the source IP address 1.1.1.1.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule deny source 1.1.1.1 0
```

rule (in advanced IPv4 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *dest-addr dest-wildcard* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **established** | **fragment** | **icmp-type** { *icmp-type icmp-code* | *icmp-message* } | **logging** | **precedence** *precedence* | **reflective** | **source** { *sour-addr sour-wildcard* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-name* | **tos** *tos* | **vpn-instance** *vpn-instance-name*] *

undo rule *rule-id* [**destination** | **destination-port** | **dscp** | **established** | **fragment** | **icmp-type** | **logging** | **precedence** | **reflective** | **source** | **source-port** | **time-range** | **tos** | **vpn-instance**] *

View Advanced IPv4 ACL view

Parameter *rule-id*: Advanced IPv4 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

protocol: Protocol carried by IP. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmp** (1), **igmp** (2), **ip**, **ipinip** (4), **ospf** (89), **tcp** (6), **udp** (17).

Table 546 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
source { sour-addr sour-wildcard | **any** }	Specifies a source address.	The sour-addr sour-wildcard argument specifies a source IP address in dotted decimal notation. Setting the wildcard to a zero indicates a host address. The **any** keyword indicates any source IP address.
destination { dest-addr dest-wildcard | **any** }	Specifies a destination address.	The dest-addr dest-wildcard argument specifies a destination IP address in dotted decimal notation. Setting the dest-wildcard to a zero indicates a host address. The **any** keyword indicates any destination IP address.
precedence precedence	Specifies an IP precedence value.	The precedence argument can be a number in the range 0 to 7, or in words, **routine**, **priority**, **immediate**, **flash**, **flash-override**, **critical**, **internet**, or **network**.
tos tos	Specifies a ToS preference.	The tos argument can be a number in the range 0 to 15, or in words, **max-reliability** (2), **max-throughput** (4), **min-delay** (8), **min-monetary-cost** (1), or **normal** (0).
dscp dscp	Specifies a DSCP priority.	The dscp argument can be a number in the range 0 to 63, or in words, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
logging	Specifies to log matched packets.	The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.

Table 546 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
reflective	Specifies the rule to be reflective.	A rule with the **reflective** keyword can be defined only for TCP, UDP, or ICMP packets and its statement can only be **permit**.
vpn-instance *vpn-instance-name*	Specifies a VPN instance.	The *vpn-instance-name* argument is a case-sensitive string of 1 to 31 characters.
fragment	Indicates that the rule applies only to non-first fragments.	With this keyword not provided, the rule is effective to both non-fragments and fragments.
time-range time-name	Specifies the time range in which the rule can take effect.	The time-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp**, you may define the parameters in the following table.

Table 547 TCP/UDP-specific parameters for advanced IPv4 ACL rules

Parameter	Function	Description
source-port operator port1 [port2]	Defines a UDP or TCP source port against which UDP or TCP packets are matched.	The operator argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), **neq** (not equal to), and **range** (inclusive range). port1, port2: TCP or UDP port number, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), or **www** (80). UDP port number can be represented in words as follows: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177).
destination-port operator port1 [port2]	Defines a UDP or TCP destination port against which UDP or TCP packets are matched.	
established	Defines the rule for TCP connection packets.	A keyword specific to TCP. On a router, With this keyword, the rule matches the TCP connection packets with the ACK or RST flag.

If the *protocol* argument is set to **icmp**, you may define the parameters in the following table.

Table 548 Parameters for advanced IPv4 ACL rules

Parameter	Function	Description
icmp-type { *icmp-type* *icmp-code* | *icmp-message* }	Specifies the ICMP message type and code.	The *icmp-type* argument ranges from 0 to 255. The *icmp-code* argument ranges from 0 to 255. The *icmp-message* argument specifies a message name. For available ICMP messages, see Table 549.

The following table provides the ICMP messages that you can specify in advanced IPv4 ACL rules.

Table 549 ICMP messages and their codes

ICMP message	Type	Code
echo	8	0
echo-reply	0	0
fragmentneed-DFset	3	4
host-redirect	5	1
host-tos-redirect	5	3
host-unreachable	3	1
information-reply	16	0
information-request	15	0
net-redirect	5	0
net-tos-redirect	5	2
net-unreachable	3	0
parameter-problem	12	0
port-unreachable	3	3
protocol-unreachable	3	2
reassembly-timeout	11	1
source-quench	4	0
source-route-failed	3	5
timestamp-reply	14	0
timestamp-request	13	0
ttl-exceeded	11	0

Description Use the **rule** command to define or modify an advanced IPv4 ACL rule. If the rule does not exist, it is created first.

Use the **undo rule** command to remove an advanced ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.

Example # Define a rule to permit the TCP packets to pass with the destination port 80 sent from 129.9.0.0 to 202.38.160.0.

```
<Sysname> system-view
[Sysname] acl number 3101
[Sysname-acl-adv-3101] rule permit tcp source 129.9.0.0 0.0.255.255
destination 202.38.160.0 0.0.0.255 destination-port eq 80
```

rule (in Ethernet frame header ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**cos** *vlan-pri* | **dest-mac** *dest-addr dest-mask* | **lsap** *lsap-code lsap-wildcard* | **source-mac** *sour-addr source-mask* | **time-range** *time-name* | **type** *type-code type-wildcard*] *

undo rule *rule-id*

View Ethernet frame header ACL view

Parameter *rule-id*: Ethernet frame header ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

cos *vlan-pri:* Defines an 802.1p priority. The *vlan-pri* argument takes a value in the range 0 to 7; or its equivalent in words, **best-effort**, **background**, **spare**, **excellent-effort**, **controlled-load**, **video**, **voice**, or **network-management**.

dest-mac *dest-addr dest-mask:* Specifies a destination MAC address range. The *dest-addr* and *dest-mask* arguments indicate a destination MAC address and mask in xxxx-xxxx-xxxx format.

lsap *lsap-code lsap-wildcard:* Defines the DSAP and SSAP fields in the LLC encapsulation. The *lsap-code* argument is a 16-bit hexadecimal number indicating frame encapsulation. The *lsap-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard of the LSAP code.

source-mac *sour-addr source-mask:* Specifies a source MAC address range. The *sour-addr* and *sour-mask* arguments indicate a source MAC address and mask in xxxx-xxxx-xxxx format.

time-range *time-name:* Specifies the time range in which the rule can take effect. The *time-name* argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

type *type-code type-wildcard:* Defines a link layer protocol. The *type-code* argument is a 16-bit hexadecimal number indicating frame type. It is corresponding to the type-code field in Ethernet_II and Ethernet_SNAP frames. The *type-wildcard* argument is a 16-bit hexadecimal number indicating the wildcard.

The use of this parameter depends on the hardware chip of your device.

Description Use the **rule** command to create an Ethernet frame header ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an Ethernet frame header ACL rule.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl** command to verify rules configured in an ACL. If the match order for this ACL is **auto**, rules are displayed in the depth-first order rather than by rule number.

Example # Create a rule to deny packets with the 802.1p priority of 3.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule deny cos 3
```

rule (in user-defined ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [{ **l2** *rule-string rule-mask offset* }&<1-8>] [**time-range** *time-name*]

undo rule *rule-id*

View User-defined ACL view

Parameter *rule-id*: User-defined ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

l2: Sets the offset from the beginning of the Layer 2 frame header.

time-range *time-name*: Specifies the time range in which the rule can take effect. The *time-name* argument is a case-insensitive string of 1 to 32 characters. The name must begin with an English letter and cannot be all to avoid confusion.

rule-string: Defines a match pattern in hexadecimal format. Its length must be a multiple of two.

rule-mask: Defines a match pattern mask in hexadecimal format. Its length must be the same as that of the match pattern.

offset: The offset in bytes at which the match operation begins.

&<1-8>: Indicates that up to eight match patterns can be defined in the rule.

Description Use the **rule** command to create a user-defined IPv4 ACL rule.

Use the **undo rule** command to remove a user-defined ACL rule.

You will fail to create or modify a user-defined ACL rule if its permit/deny statement is exactly the same as another rule.

When defining user-defined ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in rule numbering steps of five. A rule ID thus assigned is greater than the current highest rule ID. For example, if the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl** command to verify rules configured in an ACL.

The support to this command varies by device.

Example # Create a user-defined ACL rule.

```
<Sysname> system-view
[Sysname] acl number 5005
[Sysname-acl-user-5005] rule 0 permit l2 0806 ffff 20
```

rule comment (for IPv4)

Syntax **rule** *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view, user-defined ACL view

Parameter *rule-id*: IPv4 ACL rule number in the range 0 to 65534.

text: IPv4 ACL rule description, a string of up to 127 characters.

Description Use the **rule comment** command to create or modify an ACL rule description, for example to describe the purpose of the ACL rule or the parameters it contains.

You will fail to do that if the specified rule does not exist.

Use the **undo rule comment** command to remove the ACL rule description.

By default, no rule description is created.

Example # Create a rule in ACL 2000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule 0 deny source 1.1.1.1 0
[Sysname-acl-basic-2000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 3000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] rule 0 permit ip source 1.1.1.1 0
[Sysname-acl-adv-3000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 4000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] rule 0 deny cos 3
[Sysname-acl-ethernetframe-4000] rule 0 comment This rule is used in eth 1
```

Create a rule in ACL 5000 and define the rule description.

```
<Sysname> system-view
[Sysname] acl number 5000
[Sysname-acl-user-5000] rule 0 permit l2 14 20 10
[Sysname-acl-user-5000] rule 0 comment This rule is used in eth 1
```

step (for IPv4)

Syntax **step** *step-value*

undo step

View Basic IPv4 ACL view, advanced IPv4 ACL view, Ethernet frame header ACL view

Parameter *step-value*: IPv4 ACL rule numbering step, in the range 1 to 20.

Description Use the **step** command to set a rule numbering step.

Use the **undo step** command to restore the default.

By default, rule numbering step is five.

When defining rules in an IPv4 ACL, you do not necessarily assign them numbers. The system can do this automatically in steps. For example, if the default step applies, rules you created are automatically numbered 0, 5, 10, 15, and so on. One benefit of rule numbering step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, 15 in an ACL configured with the step of five, you can still insert a rule numbered 1.

Any step change can result in renumbering. For example, after you change the step in the above example from five to two, the rules are renumbered 0, 2, 4, 6, and 8.

Note that even if the current step is the default, performing the **undo step** command can still result in rule renumbering. Suppose that ACL 3001 adopts the default numbering step and contains two rules numbered 0 and 5. After you insert rule 1 and rule 3, the rules are numbered 0, 1, 3, and 5. If you perform the **undo step** command, they will be renumbered 0, 5, 10, and 15.

Example # Set the rule numbering step to 2 for ACL 2000.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] step 2
```

Set the rule numbering step to 2 for ACL 3000.

```
<Sysname> system-view
[Sysname] acl number 3000
[Sysname-acl-adv-3000] step 2
```

Set the rule numbering step to 2 for ACL 4000.

```
<Sysname> system-view
[Sysname] acl number 4000
[Sysname-acl-ethernetframe-4000] step 2
```

139
IPv6 ACL Configuration Commands

acl ipv6

Syntax **acl ipv6 number** *acl6-number* [**name** *acl6-name*] [**match-order** { **auto** | **config** }]

undo acl ipv6 { **all** | **name** *acl6-name* | **number** *acl6-number* }

View System view

Parameter *acl6-number*: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs
- 10000 to 42767 for simple IPv6 ACLs

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

match-order: Sets the order in which ACL rules are matched.

- **auto**: Performs depth-first match. For how depth-first match works, refer to the "IPv6 ACL Match Order" section in accompanied *ACL Configuration*.
- **config**: Performs matching against rules in the order in which they are configured.

all: All IPv6 ACLs.

Description Use the **acl ipv6** command to enter IPv6 ACL view. If the ACL does not exist, it is created first.

Use the **undo acl ipv6** command to remove a specified or all IPv6 ACLs.

By default, the match order is **config**.

Note that:

- The match order setting is not available for simple IPv6 ACLs, because a simple IPv6 ACL can contain only one rule.

- You can specify a name for an IPv6 ACL only when you create the ACL. After creating an ACL, you cannot specify a name for it, nor can you change or remove the name of the ACL.
- The name of an IPv6 ACL must be unique among IPv6 ACLs. However, an IPv4 ACL and an IPv6 ACL can share the same name.
- If you specify both an ACL number and an ACL name in one command to enter the view of an existing ACL, be sure that the ACL number and ACL name identify the same ACL.
- A simple IPv6 ACL cannot have any name. When creating a simple IPv6 ACL, you cannot specify the **name** *acl6-name* combination.
- You can also use this command to modify the match order of an existing IPv6 ACL but only when it is empty.

Example # Create IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

Create IPv6 ACL 2002, giving the ACL a name of flow.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002 name flow
[Sysname-acl6-basic-2002-flow]
```

Enter the view of an IPv6 ACL that has no name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000]
```

Enter the view of an IPv6 ACL that has a name by specifying its number.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2002
[Sysname-acl6-basic-2002-flow]
```

Delete the IPv6 ACL with the number of 2000.

```
<Sysname> system-view
[Sysname] undo acl ipv6 number 2000
```

Delete the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] undo acl ipv6 name flow
```

acl ipv6 copy

Syntax **acl ipv6 copy** { *source-acl6-number* | **name** *source-acl6-name* } **to** { *dest-acl6-number* | **name** *dest-acl6-name* }

View **System view**

Parameter *source-acl6-number*: Number of an existing IPv6 ACL, which must be in the following ranges (the available ACL number ranges varies by device):

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

source-acl6-name: Name of an existing IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

dest-acl6-number: Number of a non-existent IPv6 ACL, which must be in the following ranges (the available ACL number ranges varies by device):

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

dest-acl6-name: Name for the new IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion. The system will automatically assign the new ACL a sequence number which is the smallest one among the available ones in the ACL range for the ACL type.

Description Use the **acl ipv6 copy** command to copy an existent IPv6 ACL (namely, the source IPv6 ACL) to generate a new one (namely, the destination IPv6 ACL), which is of the same type and has the same match order, match rules, rule numbering step and descriptions.

Note that:

- The source IPv6 ACL and the destination IPv6 ACL must be of the same type.
- The generated ACL does not take the name of the source IPv4 ACL.
- A simple IPv6 ACL does not support this feature.

Example # Copy ACL 2008 to generate ACL 2009.

```
<Sysname> system-view
[Sysname] acl ipv6 copy 2008 to 2009
```

acl ipv6 name

Syntax **acl ipv6 name** *acl6-name*

View System view

Parameter *acl6-name*: Name of the IPv6 ACL, a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description Use the **acl ipv6 name** command to enter the view of an existing IPv6 ACL by specifying its name.

Example # Enter the view of the IPv6 ACL named flow.

```
<Sysname> system-view
[Sysname] acl ipv6 name flow
[Sysname-acl6-basic-2002-flow]
```

description (for IPv6)

Syntax **description** *text*

undo description

View Basic IPv6 ACL view, advanced IPv6 ACL view, simple IPv6 ACL view

Parameter *text*: ACL description, a case-sensitive string of 1 to 127 characters.

Description Use the **description** command to create an IPv6 ACL description, to describe the purpose of the ACL for example.

Use the **undo description** command to remove the IPv6 ACL description.

By default, an IPv6 ACL has no description configured.

Example # Create a description for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] description This acl is used in eth 0
```

Create a description for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] description This acl is used in eth 0
```

Create a description for IPv6 ACL 10000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 10000
[Sysname-acl6-simple-10000] description This acl is used in eth 0
```

display acl ipv6

Syntax **display acl ipv6** { *acl6-number* | **all** | **name** *acl6-name* }

View Any view

Parameter *acl6-number*: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs
- 10000 to 42767 for simple IPv6 ACLs

all: All IPv6 ACLs.

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description Use the **display acl ipv6** command to display information about specified or all IPv6 ACLs.

The output will be displayed in matching order.

Example # Display information about IPv6 ACL 2001.

```
<Sysname> display acl ipv6 2001
Basic IPv6 ACL  2001, named flow, 1 rule,
Acl’s step is 5
rule 0 permit source 1::2/128 (0 times matched)
rule 0 comment This rule is used in eth 1
```

Table 550 Description on the fields of the display acl ipv6 command

Field	Description
Basic IPv6 ACL 2001	The displayed information is about the basic IPv4 ACL 2001.
named flow	The name of the ACL is flow.
1 rule	The ACL contains one rule.
Acl’s step is 5	The rules in this ACL are numbered in steps of 5.
5 times matched	Five matches for the rule. Only ACL matches performed by software are counted. The field appears as long as one match is found.
rule 0 comment This rule is used in eth 1	The description of ACL rule 5 is "This rule is used in eth 1."

reset acl ipv6 counter

Syntax **reset acl ipv6 counter** { *acl6-number* | **all** | **name** *acl6-name* }

View User view

Parameter **all**: All basic and advanced IPv6 ACLs.

acl6-number: IPv6 ACL number. It is a value in one of the following ranges:

- 2000 to 2999 for basic IPv6 ACLs
- 3000 to 3999 for advanced IPv6 ACLs

name *acl6-name*: Specifies the name of the ACL, which is a case insensitive string of 1 to 32 characters. It must start with an English letter and cannot be the English word of all to avoid confusion.

Description Use the **reset acl ipv6 counter** command to clear statistics about specified or all basic and advanced IPv6 ACLs.

Example # Clear the statistics about IPv6 ACL 2001.

```
<Sysname> reset acl ipv6 counter 2001
```

Clear the statistics about the IPv6 ACL named flow.

```
<Sysname> reset acl ipv6 counter name flow
```

rule (in basic IPv6 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } [**fragment** | **logging** | **source** { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** } | **time-range** *time-name*] *

undo rule *rule-id* [**fragment** | **logging** | **source** | **time-range**] *

View Basic IPv6 ACL view

Parameter *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

fragment: Indicates that the rule applies only to non-first fragments. The rule applies to both fragments and non-fragments without this keyword.

logging: Specifies to log matched packets. The log provides information about ACL rule number, whether packets are permitted or dropped, upper layer protocol that IP carries, source/destination address, source/destination port number, and number of packets.

source { *ipv6-address prefix-length* | *ipv6-address/prefix-length* | **any** }: Specifies a source address. The *ipv6-address* and *prefix-length* arguments specify a source IPv6 address, and its address prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.

time-range *time-name:* Specifies the time range in which the rule takes effect. The *time-name* argument specifies a time range name with 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

Description Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is five and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl ipv6** command to verify rules configured in an ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Example # Create rules in IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 8 deny source fe80:5060::8050/96
```

rule (in advanced IPv6 ACL view)

Syntax **rule** [*rule-id*] { **deny** | **permit** } *protocol* [**destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **fragment** | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **logging** | **source** { *source source-prefix* | *source/source-prefix* | **any** } | **source-port** *operator port1* [*port2*] | **time-range** *time-name*] *

undo rule *rule-id* [**destination** | **destination-port** | **dscp** | **fragment** | **icmpv6-type** | **logging** | **source** | **source-port** | **time-range**] *

View Advanced IPv6 ACL view

Parameter *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

deny: Defines a deny statement to drop matched packets.

permit: Defines a permit statement to allow matched packets to pass.

protocol: Protocol carried on IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), **udp** (17).

Table 551 Match criteria and other rule information for advanced IPv6 ACL rules

Parameter	Function	Description
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source* and *source-prefix* arguments specify an IPv6 source address and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest* and *dest-prefix* arguments specify a destination IPv6 address, and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 destination address.
dscp *dscp*	Specifies a DSCP preference	The *dscp* argument can be a number in the range 0 to 63, or in words, **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, **default**, or **ef**.
logging	Specifies to log matched packets	The log provides information about ACL rule number, whether packets are permitted or denied, protocol that IP carries, source/destination IPv6 address, source/destination port number, and number of packets.
fragment	Indicates that the rule applies only to non-first fragments	With this keyword not provided, the rule is effective to both non-fragments and fragments.
time-range *time-name*	Specifies the time range in which the rule can take effect.	The time-name argument comprises 1 to 32 characters. It is case insensitive and must start with an English letter. To avoid confusion, this name cannot be all.

If the *protocol* argument is set to **tcp** or **udp,** you may define the parameters in the following table.

Table 552 TCP/UDP-specific match criteria for advanced IPv6 ACL rules

Parameter	Function	Description
source-port operator port1 [port2]	Defines the source port in the UDP/TCP packet.	The operator argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), or **range** (inclusive range).
destination-port operator port1 [port2]	Defines the destination port in the UDP/TCP packet.	The port1 and port2 arguments each specify a TCP or UDP port, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows: **chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), or **www** (80). UDP port number can be represented in words as follows: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177).

If the *protocol* argument is set to ICMPv6, you may define the parameters in the following table.

Table 553 ICMPv6-specific match criteria for advanced IPv6 ACL rules

Parameter	Function	Description
icmpv6-type { *icmpv6-type icmpv6-code* | *icmpv6-message* }	Specifies the ICMPv6 message type and code	The *icmpv6-type* argument ranges from 0 to 255. The *icmpv6-code* argument ranges from 0 to 255. The *icmpv6-message* argument specifies a message name. For available ICMPv6 messages, see Table 553

The following table provides the ICMPv6 messages that you can specify in advanced IPv6 ACL rules.

Table 554 Available ICMPv6 messages

ICMPv6 message	Type	Code
redirect	137	0
echo-request	128	0
echo-reply	129	0
err-Header-field	4	0
frag-time-exceeded	3	1
hop-limit-exceeded	3	0
host-admin-prohib	1	1
host-unreachable	1	3

Table 554 Available ICMPv6 messages

ICMPv6 message	Type	Code
neighbor-advertisement	136	0
neighbor-solicitation	135	0
network-unreachable	1	0
packet-too-big	2	0
port-unreachable	1	4
router-advertisement	134	0
router-solicitation	133	0
unknown-ipv6-opt	4	2
unknown-next-hdr	4	1

Description Use the **rule** command to create an IPv6 ACL rule or modify the rule if it has existed.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

You will fail to create or modify a rule if its permit/deny statement is exactly the same as another rule. In addition, if the ACL match order is set to **auto** rather than **config**, you cannot modify ACL rules.

When defining ACL rules, you need not assign them IDs. The system can automatically assign rule IDs, starting with 0 and increasing in certain rule numbering steps. A rule ID thus assigned is greater than the current highest rule ID. For example, if the rule numbering step is 5 and the current highest rule ID is 28, the next rule will be numbered 30. For detailed information about step, refer to "step (for IPv4)" on page 2100 and "step (for IPv6)" on page 2116.

You may use the **display acl ipv6** command to verify rules configured in an IPv6 ACL. If the match order for this IPv6 ACL is **auto**, rules are displayed in the depth-first match order rather than by rule number.

Example # Create a rule in IPv6 ACL 3000 to permit the TCP packets with the source address 2030:5060::9050/64 to pass.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule permit tcp source 2030:5060::9050/64
```

rule (in simple IPv6 ACL view)

Syntax **rule** *protocol* [**addr-flag** *addr-flag* | **destination** { *dest dest-prefix* | *dest/dest-prefix* | **any** } | **destination-port** *operator port1* [*port2*] | **dscp** *dscp* | **frag-type** { **fragment** | **fragment-subseq** | **non-fragment** | **non-subseq** } | **icmpv6-type** { *icmpv6-type icmpv6-code* | *icmpv6-message* } | **source** { *source source-prefix* | *source/source-prefix* |

any } | **source-port** *operator port1* [*port2*] | **tcp-type** { **tcpurg** | **tcpack** | **tcppsh** | **tcprst** | **tcpsyn** | **tcpfin** }] *

undo rule [**addr-flag** | **destination** | **destination-port** | **dscp** | **frag-type** | **icmp6-type** | **source** | **source-port** | **tcp-type**] *

View Simple IPv6 ACL view

Parameter *protocol*: Protocol carried on IPv6. It can be a number in the range 0 to 255, or in words, **gre** (47), **icmpv6** (58), **ipv6**, **ipv6-ah** (51), **ipv6-esp** (50), **ospf** (89), **tcp** (6), **udp** (17).

Table 555 Parameters for simple IPv6 ACL rules

Parameter	Function	Description
addr-flag *addr-flag*	Specifies an IPv6 source-destination address combination mode.	The *addr-flag* argument ranges from 1 to 6, where 1 = 64-bit source address prefix + 64 destination address prefix 2 = 64-bit source address prefix + 64-bit destination address suffix 3 = 64-bit source address suffix + 64-bit destination address prefix 4 = 64-bit source address suffix + 64-bit destination address suffix 5 = 128-bit source address 6 = 128-bit destination address
source { *source source-prefix* | *source/source-prefix* | **any** }	Specifies a source IPv6 address.	The *source* and *source-prefix* arguments specify an IPv6 source address, and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 source address.
destination { *dest dest-prefix* | *dest/dest-prefix* | **any** }	Specifies a destination IPv6 address.	The *dest* and *dest-prefix* arguments specify an IPv6 destination address and its prefix length in the range 1 to 128. The **any** keyword indicates any IPv6 destination address.
frag-type { **fragment** | **fragment-subseq** | **non-fragment** | **non-subseq** }	Indicates to which type of fragment the rule applies.	The **fragment** keyword indicates that the rule applies only to first fragments. The **fragment-subseq** keyword indicates that the rule applies only to non-first fragments. The **non-fragment** keyword indicates that the rule applies only to unfragmented packets. The **non-subseq** keyword indicates that the rule applies only to last fragments.
dscp *dscp*	Specifies the DSCP preference	The *dscp* argument ranges from 0 to 63.

If the *protocol* argument is set to **tcp** or **udp,** you may define the parameters in the following table.

Table 556 TCP/UDP-specific parameters for simple IPv6 ACL rules

Parameter	Function	Description
source-port *operator port1* [*port2*]	Defines a UDP or TCP source port against which UDP or TCP packets are matched.	The *operator* argument can be **lt** (lower than), **gt** (greater than), **eq** (equal to), and **range** (inclusive range). The *port1* and *port2* arguments each specify a TCP or UDP port, represented by a number in the range 0 to 65535. TCP port number can be represented in words as follows:
destination-port *operator port1* [*port2*]	Defines a UDP or TCP destination port against which UDP or TCP packets are matched.	**chargen** (19), **bgp** (179), **cmd** (514), **daytime** (13), **discard** (9), **domain** (53), **echo** (7), **exec** (512), **finger** (79), **ftp** (21), **ftp-data** (20), **gopher** (70), **hostname** (101), **irc** (194), **klogin** (543), **kshell** (544), **login** (513), **lpd** (515), **nntp** (119), **pop2** (109), **pop3** (110), **smtp** (25), **sunrpc** (111), **tacacs** (49), **talk** (517), **telnet** (23), **time** (37), **uucp** (540), **whois** (43), or **www** (80) UDP port number can be represented in words as follows: **biff** (512), **bootpc** (68), **bootps** (67), **discard** (9), **dns** (53), **dnsix** (90), **echo** (7), **mobilip-ag** (434), **mobilip-mn** (435), **nameserver** (42), **netbios-dgm** (138), **netbios-ns** (137), **netbios-ssn** (139), **ntp** (123), **rip** (520), **snmp** (161), **snmptrap** (162), **sunrpc** (111), **syslog** (514), **tacacs-ds** (65), **talk** (517), **tftp** (69), **time** (37), **who** (513), **xdmcp** (177).
tcp-type { **tcpurg** | **tcpack** | **tcppsh** | **tcprst** | **tcpsyn** | **tcpfin** }	Defines a TCP flag.	Available only when the *protocol* argument is set to TCP.

If the *protocol* argument is set to ICMPv6, you may define the parameters in the following table.

Table 557 ICMPv6-specific parameters for simple IPv6 ACL rules

Parameter	Function	Description
icmpv6-type { *icmpv6-type icmpv6-code* | *icmpv6-message* }	Specifies a ICMPv6 message type and code	The *icmpv6-type* argument ranges from 0 to 255. The *icmpv6-code* argument ranges from 0 to 255. The *icmpv6-message* argument specifies a message name. For available ICMPv6 messages, see Table 558.

The following table provides the ICMPv6 messages that you can specify in simple IPv6 ACL rules.

Table 558 ICMPv6 messages definable in simple IPv4 ACL rules

ICMPv6 message	ICMPv6 TYPE	ICMPv6 CODE
redirect	Type=137	Code=0
echo-request	Type=128	Code=0
echo-reply	Type=129	Code=0
err-Header-field	Type=4	Code=0
frag-time-exceeded	Type=3	Code=1
hop-limit-exceeded	Type=3	Code=0
host-admin-prohib	Type=1	Code=1
host-unreachable	Type=1	Code=3

Table 558 ICMPv6 messages definable in simple IPv4 ACL rules

ICMPv6 message	ICMPv6 TYPE	ICMPv6 CODE
neighbor-advertisement	Type=136	Code=0
neighbor-solicitation	Type=135	Code=0
network-unreachable	Type=1	Code=0
packet-too-big	Type=2	Code=0
port-unreachable	Type=1	Code=4
router-advertisement	Type=134	Code=0
router-solicitation	Type=133	Code=0
unknown-ipv6-opt	Type=4	Code=2
unknown-next-hdr	Type=4	Code=1

Description Use the **rule** command to create an IPv6 ACL rule.

Use the **undo rule** command to remove an IPv6 ACL rule or parameters from the rule.

With the **undo rule** command, if no parameters are specified, the entire ACL rule is removed; if other parameters are specified, only the involved information is removed.

Support for this command varies by device.

Example # Create a rule in IPv6 ACL 10000 to match the TCP RST packets with the source address of 2200::100/64.

```
<Sysname> system-view
[Sysname] acl ipv6 number 10000
[Sysname-acl6-simple-10000] rule tcp addr-flag 4 source 2200::100/64
 tcp-type tcprst
```

rule comment (for IPv6)

Syntax **rule** *rule-id* **comment** *text*

undo rule *rule-id* **comment**

View Basic IPv6 ACL view, advanced IPv6 ACL view

Parameter *rule-id*: IPv6 ACL rule number in the range 0 to 65534.

text: IPv6 ACL rule description, a case-sensitive string of 1 to 127 characters.

Description Use the **rule comment** command to create or modify a description for an existing IPv6 ACL rule, for example to describe the purpose of the ACL rule or its attributes.

Use the **undo rule comment** command to remove the IPv6 ACL rule description.

By default, no rule description is created.

Example # Define a rule in IPv6 ACL 2000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] rule 0 permit source 2030:5060::9050/64
[Sysname-acl6-basic-2000] rule 0 comment This rule is used in eth 1
```

Define a rule in IPv6 ACL 3000 and create a description for the rule.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] rule 0 permit tcp source 2030:5060::9050/64
[Sysname-acl6-adv-3000] rule 0 comment This rule is used in eth 1
```

step (for IPv6)

Syntax **step** *step-value*

undo step

View Basic IPv6 ACL view, advanced IPv6 ACL view

Parameter *step-value*: The step in which the rules in the IPv6 ACL is numbered, in the range 1 to 20.

Description Use the **step** command to set a rule numbering step for the IPv6 ACL.

Use the **undo step** command to restore the default.

By default, the rule numbering step is five.

When defining rules in an IPv6 ACL, you do not necessarily assign them numbers. The system can do this automatically in steps. For example, if the default step applies, rules you created are numbered 0, 5, 10, 15, and so on automatically.

One benefit of rule numbering step is that it allows you to insert new rules between existing ones as needed. For example, after creating four rules numbered 0, 5, 10, 15 in an ACL configured with the step of 5, you can still insert a rule numbered 1.

Any step change can result in renumbering. For example, after you change the step in the above example from 5 to 2, the rules are renumbered 0, 2, 4, 6, and 8.

Note that even if the current step is the default, performing the **undo step** command can still result in rule renumbering. Suppose that IPv6 ACL 3001 adopts the default numbering step and contains two rules numbered 0 and 5. After you insert rule 1 and rule 3, the rules are numbered 0, 1, 3, and 5. If you perform the **undo step** command, they will be renumbered 0, 5, 10, and 15.

Example # Set the rule numbering step to 2 for IPv6 ACL 2000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2000
[Sysname-acl6-basic-2000] step 2
```

Set the rule numbering step to 2 for IPv6 ACL 3000.

```
<Sysname> system-view
[Sysname] acl ipv6 number 3000
[Sysname-acl6-adv-3000] step 2
```

140 IPSEC CONFIGURATION COMMANDS

ah authentication-algorithm

Syntax **ah authentication-algorithm** { **md5** | **sha1** }

undo ah authentication-algorithm

View IPSec proposal view

Parameter **md5**: Uses MD5.

sha1: Uses SHA1.

Description Use the **ah authentication-algorithm** command to specify the authentication algorithm for the authentication header (AH) protocol.

Use the **undo ah authentication-algorithm** command to restore the default.

By default, MD5 is used.

Note that you need to use the **transform** command to specify the security protocol as AH or both AH and ESP before specifying the authentication algorithm for AH.

Related command: **ipsec proposal** and **transform**.

Example # Configure IPSec proposal prop1 to use AH and SHA1.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform ah
[Sysname-ipsec-proposal-prop1] ah authentication-algorithm sha1
```

cryptoswitch fabric enable

Syntax **cryptoswitch fabric enable**

undo cryptoswitch fabric enable

View System view

Parameter None

Description Use the **cryptoswitch fabric enable** command to enable the encryption switch fabric.

Use the **undo cryptoswitch fabric enable** command to disable the encryption switch fabric.

- If an encryption card is bound, IPSec processing is performed by the card as long as it works properly. If the encryption card fails, the encryption switch fabric cannot automatically substitute the encryption card for IPSec processing even the encryption switch fabric is enabled. This is also the case for the IPSec module backup function. In this case, the matched packets are discarded until you manually remove the binding between an IPSec policy (group) and an encryption card.

If no encryption card is bound, there are also two cases:

- If the encryption switch fabric is enabled, it takes over the responsibility of IPSec processing;
- If the encryption switch fabric is disabled or has failed but the IPSec module backup function is enabled, the IPSec module takes over the responsibility of IPSec processing; if the IPSec module backup function is disabled, the matched packets are discarded.

By default, the encryption switch fabric is enabled.

Example # Enable the encryption switch fabric.

```
<Sysname> system-view
[Sysname] cryptoswitch fabric enable
```

display encrypt-card fast-switch

Syntax **display encrypt-card fast-switch**

View Any view

Parameter None

Description Use the **display encrypt-card fast-switch** command to display the contents of the encryption card fast switching cache.

Parameter # Display the contents of the encryption card fast switching cache.

```
<sysname> display encrypt-card fast-switch
encrypt-card Fast-Forwarding cache: (200 times matched)
-------------------------------------------------------------------------
Index   SourIP    SourPort   DestIP   DestPort  Prot    TdbID      ENC/DEC
38     11.1.1.1      8      11.1.1.2     0       1    0x00000002   encrypt
139    11.1.1.2      0      11.1.1.1     0       50   0x00000001   decrypt
```

Table 559 Description on the fields of the display encrypt-card fast-switch command

Field	Description
encrypt-card Fast-Forwarding cache	Encryption card fast forwarding cache
Index	Index number of the encryption card fast forwarding entry
SourIP	Source IP address of the data flow
SourPort	Source port number of the data flow
DestIP	Destination IP address of the data flow
DestPort	Destination port number of the data flow
Prot	Protocol number
TdbID	Identification of the SA
ENC/DEC	Action on the data flow, encryption or decryption

display ipsec policy

Syntax **display ipsec policy** [**brief** | **name** *policy-name* [*seq-number*]]

View Any view

Parameter **brief**: Displays brief information about all the IPSec policies.

name: Displays detailed information about a specified IPSec policy or IPSec policy group.

policy-name: Name of the IPSec policy, a string of 1 to 15 characters.

seq-number: Sequence number of the IPSec policy, in the range 1 to 10000.

Description Use the **display ipsec policy** command to display information about IPSec policies.

Note that:

- If you do not specify any keywords or parameters, the command displays detailed information about all IPSec policies.
- If you specify the **name** *policy-name* combination but leave the *seq-number* argument, the command displays detailed information about the specified IPSec policy group.

Related command: **ipsec policy (system view)**.

Example # Display brief information about all IPSec policies.

```
<Sysname> display ipsec policy brief
IPsec-Policy-Name     Mode    acl          ike-peer name
------------------------------------------------------------------------
map-1                 isakmp  3000         peerr1234567890
map-3                 template
mappp1234567890-1     isakmp  3000         peer
mappp5432167890-1     template
```

```
mapss1234567890-10000 isakmp               peerr1234567890

IPsec-Policy-Name     Mode    acl          Local-Address  Remote-Address
------------------------------------------------------------------------
map-2                 manual  3000        255.255.255.255 255.255.255.255
mappp0123456789-1     manual  3000
```

Table 560 Description on the fields of the display ipsec policy brief command

Field	Description
IPsec-Policy-Name	Name and sequence number of the IPSec policy separated by hyphen
Mode	Negotiation mode of the IPSec policy
acl	Access control list referenced by the IPSec policy
ike-peer name	IKE peer name
Local-Address	IP address of the local end
Remote-Address	IP address of the remote end

Display detailed information about all IPSec policies

```
<Sysname> display ipsec policy
==========================================
IPsec Policy Group: "policy_isakmp"
Using interface: {Ethernet1/0}
==========================================

  ------------------------------------
  IPsec policy name: "policy_isakmp"
  sequence number: 10
  mode: isakmp
  ------------------------------------
    security data flow : 100
    tunnel remote address: 162.105.10.2
    perfect forward secrecy: None
    proposal name: prop1
    ipsec sa local duration(time based): 3600 seconds
    ipsec sa local duration(traffic based): 1843200 kilobytes

==========================================
IPsec Policy Group: "policy_man"
Using interface: {Ethernet1/1}
==========================================

  ----------------------------------------
  IPsec policy name: "policy_man"
  sequence number: 10
  mode: manual
  ----------------------------------------
    security data flow : 100
    tunnel local  address: 162.105.10.1
    tunnel remote address: 162.105.10.2
    proposal name: prop1
    inbound AH setting:
      AH spi: 12345 (0x3039)
      AH string-key:
      AH authentication hex key : 12345678901234567890123456789012345678901234567890
    inbound ESP setting:
      ESP spi: 23456 (0x5ba0)
      ESP string-key:
      ESP encryption hex key: 1234567890abcdef1234567890abcdef1234567812345678
      ESP authentication hex key: 1234567890abcdef1234567890abcdef
    outbound AH setting:
      AH spi: 54321 (0xd431)
      AH string-key:
      AH authtication hex key: 11223344556677889900112233445566778899001
```

```
outbound ESP setting:
  ESP spi: 65432 (0xff98)
  ESP string-key:
  ESP encryption hex key: 11223344556677889900aabbccddeeff1234567812345678
  ESP authentication hex key: 1122334455667788990aabbccddeeff
```

Table 561 Description on the fields of the display ipsec policy command

Field	Description
security data flow	Access control list referenced by the IPSec policy
proposal name	Name of the proposal referenced by the IPSec policy
inbound/outbound ah/esp setting	AH/ESP settings in the inbound/outbound direction, including the SPI and key
tunnel local address	Local IP address of the tunnel
tunnel remote address	Remote IP address of the tunnel
perfect forward secrecy	Whether PFS is enabled.

display ipsec policy-template

Syntax **display ipsec policy-template** [**brief** | **name** *template-name* [*seq-number*]]

View Any view

Parameter **brief**: Displays brief information about all the IPSec policy templates.

name: Displays detailed information about a specified IPSec policy template or IPSec policy template group.

template-name: Name of the IPSec policy template, a string of 1 to 15 characters.

seq-number: Sequence number of the IPSec policy template, in the range 1 to 10000.

Description Use the **display ipsec policy-template** command to display information about IPSec policy templates.

Note that:

- If you do not specify any keywords or parameters, the command displays detailed information about all IPSec policy templates.
- If you specify the **name** *policy-name* combination but leave the *seq-number* argument, the command displays information about the specified IPSec policy template group.

Related command: **ipsec policy-template**.

Example # Display brief information about all IPSec policy templates.

```
<Sysname> display ipsec policy-template brief
Policy-template-Name     acl            Remote-Address
```

```
-----------------------------------------------------
test-tplt300              2200
```

Table 562 Description on the fields of display ipsec policy-template brief

Field	Description
Policy-template-Name	Name and sequence number of the IPSec policy template separated by hyphen
acl	Access control list referenced by the IPSec policy template
Remote Address	Remote IP address

display ipsec proposal

Syntax **display ipsec proposal** [*proposal-name*]

View Any view

Parameter *proposal-name*: Name of a proposal, a string of 1 to 15 characters.

Description Use the **display ipsec proposal** command to display information about a specified or all IPSec proposals.

Related command: **ipsec proposal**.

Example # Display information about all IPSec proposals.

```
<Sysname> display ipsec proposal
IPsec proposal name: prop2
     encapsulation mode: tunnel
     transform: ah-new
     AH protocol: authentication sha1-hmac-96
IPsec proposal name: prop1
     encapsulation mode: transport
     transform: esp-new
     ESP protocol: authentication md5-hmac-96, encryption des
```

Table 563 Description on the fields of the display ipsec proposal command

Field	Description
IPsec proposal name	Name of the IPSec proposal
encapsulation mode	Encapsulation mode used by the IPSec proposal, transport or tunnel
transform	Transform protocol (s) used by the IPSec proposal, AH, ESP or both
AH protocol	Authentication algorithm used by AH
ESP protocol	Authentication algorithm and encryption algorithm used by ESP

display ipsec sa

Syntax **display ipsec sa** [**brief** | **duration** | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]

View Any view

Parameter **brief**: Displays brief information about all SAs.

duration: Displays the global SA lifetime information.

policy: Displays detailed information about SAs created by using a specified IPSec policy.

policy-name: Name of the IPSec policy, a string 1 to 15 characters.

seq-number: Sequence number of the IPSec policy, in the range 1 to 10000.

remote *ip-address*: Displays detailed information about the SA with a specified remote address.

Description Use the **display ipsec sa** command to display information about SAs.

With no parameter or keyword specified, the command displays information about all SAs.

Related command: **reset ipsec sa**, **ipsec sa global-duration**.

Example # Display brief information about all SAs.

```
<Sysname> display ipsec sa brief
Src Address  Dst Address  SPI    Protocol     Algorithm
-------------------------------------------------------
10.1.1.1     10.1.1.2     300    ESP          E:DES; A:HMAC-MD5-96
10.1.1.2     10.1.1.1     400    ESP          E:DES; A:HMAC-MD5-96
```

Table 564 Description on the fields of the display ipsec sa brief command

Field	Description
Src Address	Local IP address
Dst Address	Remote IP address
SPI	Security parameter index
Protocol	Security protocol used by IPSec
Algorithm	Authentication algorithm and encryption algorithm used by the security protocol, where E indicates the encryption algorithm and A indicates the authentication algorithm.

Display the global SA lifetime settings.

```
<Sysname> display ipsec sa duration
     ipsec sa global duration (traffic based): 1843200 kilobytes
     ipsec sa global duration (time based): 3600 seconds
```

Display detailed information about all SAs.

```
<Sysname> display ipsec sa
==============================
Interface: Ethernet0/0
    path MTU: 1500
==============================
```

```
-----------------------------
IPsec policy name: "r2"
sequence number: 1
mode: isakmp
-----------------------------
  connection id: 3
  encapsulation mode: tunnel
  perfect forward secrecy: None
  tunnel:
      local  address: 2.2.2.2
      remote address: 1.1.1.2
  flow:    (11 times matched)
      sour addr: 192.168.2.0/255.255.255.0  port: 0  protocol: IP
      dest addr: 192.168.1.0/255.255.255.0  port: 0  protocol: IP

  [inbound ESP SAs]
    spi: 3564837569 (0xd47b1ac1)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa remaining key duration (bytes/sec): 1887436380/2686
    max received sequence-number: 5
    udp encapsulation used for nat traversal: N

  [outbound ESP SAs]
    spi: 801701189 (0x2fc8fd45)
    proposal: ESP-ENCRYPT-DES ESP-AUTH-MD5
    sa remaining key duration (bytes/sec): 1887436380/2686
    max sent sequence-number: 6
    udp encapsulation used for nat traversal: N
```

Table 565 Description on the fields of the display ipsec sa command

Field	Description
Interface	Interface referencing the IPSec policy
path MTU	Maximum IP packet length supported by the interface
IPSec policy name	Name of the IPSec policy used
sequence number	Sequence number of the IPSec policy
mode	IPSec negotiation mode
connection id	IPSec tunnel identifier
encapsulation mode	Encapsulation mode, transport or tunnel
perfect forward secrecy	Whether the PFS is enabled.
tunnel	IPSec tunnel
local address	Local IP address of the IPSec tunnel
remote address	Remote IP address of the IPSec tunnel
flow: (11 times matched)	Number of matches of the data flow
sour addr	Source IP address of the data flow
dest addr	Destination IP address of the data flow
port	Port number
protocol	Protocol type
inbound	Information of the inbound SA
spi	Security parameter index
proposal	Security protocol and algorithms used by the IPSec proposal

Table 565 Description on the fields of the display ipsec sa command

Field	Description
sa remaining key duration	Remaining lifetime of the SA
max received sequence-number	Maximum sequence number of the received packets (relevant to the anti-replay function provided by the security protocol)
udp encapsulation used for nat traversal	Whether NAT traversal is enabled for the SA
outbound	Information of the outbound SA
max sent sequence-number	Maximum sequence number of the sent packets (relevant to the anti-replay function provided by the security protocol)

display ipsec session

Syntax **display ipsec session** [**tunnel-id** *integer*]

View Any view

Parameter *integer*: ID of the IPSec tunnel, in the range 1 to 2000000000.

Description Use the **display ipsec session** command to display information about a specified or all IPSec sessions.

IPSec can find matched tunnels directly by session, reducing the intermediate matching procedures and therefore improving the forwarding efficiency. A session is identified by the quintuplet of protocol, source IP address, source port, destination IP address, and destination port.

Related command: **reset ipsec session**.

Example # Display information about all IPSec sessions.

```
<Sysname> display ipsec session
    ------------------------------------------------------------
    total sessions : 2
    ------------------------------------------------------------
    tunnel-id : 3
    session idle time/total duration (sec) : 36/300

    session flow :      (8 times matched)
        Sour Addr : 15.15.15.1             Sour Port:    0  Protocol : 1
        Dest Addr : 15.15.15.2             Dest Port:    0  Protocol : 1

    ------------------------------------------------------------
    tunnel-id : 4
    session idle time/total duration (sec) : 7/300

    session flow :      (3 times matched)
        Sour Addr : 12.12.12.1             Sour Port:    0  Protocol : 1
        Dest Addr : 13.13.13.1             Dest Port:    0  Protocol : 1
```

Display information about the session with an IPSec tunnel ID of 5.

```
<Sysname> display ipsec session tunnel-id 5
    ------------------------------------------------------------
    total sessions : 1
    ------------------------------------------------------------
    tunnel-id : 5
    session idle duration/total duration (sec) : 30/300

    session flow :      (4 times matched)
        Sour Addr : 12.12.12.2             Sour Port:    0  Protocol : 1
        Dest Addr : 13.13.13.2             Dest Port:    0  Protocol : 1
```

Table 566 Description on the fields of the display ipsec session command

Field	Description
total sessions	Total number of IPSec sessions
tunnel-id	IPSec tunnel ID, same as the connection-id of the IPSec SA
session idle time	Idle duration of the IPSec session in seconds
total duration	Total duration of the IPSec session in seconds, defaulted to 300 seconds
session flow	Flow information of the IPSec session
times matched	Total number of packets matching the IPSec session
Sour Addr	Source IP address of the IPSec session
Dest Addr	Destination IP address of the IPSec session
Sour Port	Source port number of the IPSec session
Dest Port	Destination port number of the IPSec session
Protocol	Protocol number of the IPSec protected data flow, for example, 1 for ICMP

display ipsec statistics

Syntax **display ipsec statistics**

View Any view

Parameter None

Description Use the **display ipsec statistics** command to display IPSec packet statistics.

Related command: **reset ipsec statistics**.

Example # Display IPSec packet statistics.

```
<Sysname> display ipsec statistics
the security packet statistics:
    input/output security packets: 5124/8231
    input/output security bytes: 52348/64356
    input/output dropped security packets: 0/0
    dropped security packet detail:
      not enough memory: 0
      can't find SA: 0
      queue is full: 0
      authentication has failed: 0
      wrong length: 0
```

```
replay packet: 0
packet too long: 0
wrong SA: 0
```

Table 567 Description on the fields of the display ipsec statistics command

Field	Description
input/output security packets	Number of inbound IPSec protected packets and number of outbound IPSec protected packets
input/output security bytes	Number of inbound IPSec protected bytes and number of outbound IPSec protected bytes
input/output dropped security packets	Number of inbound IPSec protected packets that are discarded by the device and number of outbound IPSec protected packets that are discarded by the device
dropped security packet detail	Detailed information about inbound/outbound packets that get dropped
not enough memory	Number of packets dropped due to lack of memory
can't find SA	Number of packets dropped due to finding no security association
queue is full	Number of packets dropped due to full queues
authentication has failed	Number of packets dropped due to authentication failure
wrong length	Number of packets dropped due to wrong packet length
replay packet	Number of packets replayed
packet too long	Number of packets dropped due to excessive packet length
wrong SA	Number of packets dropped due to improper SA

display ipsec tunnel

Syntax **display ipsec tunnel**

View Any view

Parameter None

Description Use the **display ipsec tunnel** command to display IPSec tunnel information.

Example # Display information about IPSec tunnels.

```
<Sysname> display ipsec tunnel
    total tunnel : 1
    -----------------------------------------------
    Connection ID : 3
    Perfect forward secrecy: None
    SA's SPI :
        Inbound :  187199087 (0xb286e6f) [ESP]
        Outbound : 3562274487 (0xd453feb7) [ESP]
    Tunnel :
        Local Address:  44.44.44.44  Remote Address : 44.44.44.55
    Flow :     (8 times matched)
        Sour Addr : 44.44.44.0/255.255.255.0  Port: 0  Protocol : IP
```

```
    Dest Addr : 44.44.44.0/255.255.255.0  Port: 0  Protocol : IP
Current Encrypt-card: None
```

Table 568 Description on the fields of the display ipsec tunnel command

Field	Description
Connection ID	Connection ID, used to uniquely identify an IPSec Tunnel
Perfect forward secrecy	Perfect forward secrecy, indicating which DH group is to be used for fast negotiation mode in IKE phase 2
SA's SPI	SPIs of the inbound and outbound SAs
Tunnel	Local and remote addresses of the tunnel
Flow	Data flow protected by the IPSec tunnel, including source IP address, destination IP address, source port, destination port and protocol
Current Encrypt-card	Encryption card interface used by the current tunnel

encapsulation-mode

Syntax **encapsulation-mode** { **transport** | **tunnel** }

undo encapsulation-mode

View IPSec proposal view

Parameter **transport**: Uses transport mode.

tunnel: Uses tunnel mode.

Description Use the **encapsulation-mode** command to set the encapsulation mode (either **transport** or **tunnel**) that the security protocol uses to encapsulate IP packets.

Use the **undo encapsulation-mode** command to restore the default.

By default, a security protocol encapsulates IP packets in tunnel mode.

Related command: **ipsec proposal**.

Example # Configure IPSec proposal prop2 to encapsulate IP packets in transport mode.

```
<Sysname> system-view
[Sysname] ipsec proposal prop2
[Sysname-ipsec-proposal-prop2] encapsulation-mode transport
```

encrypt-card fast-switch

Syntax **encrypt-card fast-swtich**

undo encrypt-card fast-switch

View System view

Parameter None

Description Use the **encrypt-card fast-switch** command to enable encryption card fast switching.

Use the **undo encrypt-card fast-switch** command to disable encryption card fast switching.

By default, encryption card fast switching is disabled.

Related command: **display encrypt-card fast-switch**.

Example # Enable encryption card fast switching.

```
<sysname> system-view
[sysname] encrypt-card fast-switch
```

esp authentication-algorithm

Syntax **esp authentication-algorithm** { **md5** | **sha1** }

undo esp authentication-algorithm

View IPSec proposal view

Parameter **md5**: Uses the MD5 algorithm, which uses a 128-bit key.

sha1: Uses the SHA1 algorithm, which uses a 160-bit key.

Description Use the **esp authentication-algorithm** command to specify the authentication algorithm for ESP.

Use the **undo esp authentication-algorithm** command to configure ESP so that ESP does not perform authentication of packets.

By default, the MD5 algorithm is used.

Related command: **ipsec proposal**, **esp encryption-algorithm**, **proposal**, and **transform**.

Example # Configure IPSec proposal prop1 to use ESP and SHA1.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp authentication-algorithm sha1
```

esp encryption-algorithm

Syntax **esp encryption-algorithm** { **3des** | **aes** [*key-length*] | **des** }

undo esp encryption-algorithm

View IPSec proposal view

Parameter **3des**: Uses triple DES (3DES) in cipher block chaining (CBC) mode as the encryption algorithm. The 3DES algorithm uses a 168-bit key for encryption.

aes: Uses advanced encryption standard (AES) in CBC mode as the encryption algorithm. The AES algorithm uses a 128- bit, 192-bit, or 256-bit key for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192, and 256 and is defaulted to 128. This argument is for AES only.

des: Uses data encryption standard (DES) in CBC mode as the encryption algorithm, The DES algorithm uses a 56-bit key for encryption.

Description Use the **esp encryption-algorithm** command to specify the encryption algorithm for ESP.

Use the **undo esp encryption-algorithm** command to configure ESP so that ESP does not encrypt packets.

By default, the DES algorithm is used.

Note that:

- 3DES is well suited for environments with high demand on confidentiality and security, but it is comparatively slow in encryption. DES is enough to satisfy normal security requirements.
- ESP allows the encryption and/or authentication of a packet.
- ESP supports three IP packet protection schemes: encryption only, authentication only, or both encryption and authentication. The **undo esp encryption-algorithm** command takes effect only if no authentication algorithm is used.

Related command: **ipsec proposal**, **esp authentication-algorithm**, **proposal**, and **transform**.

Example # Configure IPSec proposal prop1 to use ESP and 3DES.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform esp
[Sysname-ipsec-proposal-prop1] esp encryption-algorithm 3des
```

ike-peer (IPSec policy view/IPSec policy template view)

Syntax **ike-peer** *peer-name*

undo ike-peer *peer-name*

View IPSec policy view/IPSec policy template view

Parameter *peer-name*: IKE peer name, a string of 1 to 15 characters.

Description Use the **ike-peer** command to reference an IKE peer in an IPSec policy or IPSec policy template configured through IKE negotiation.

Use the **undo ike peer** command to remove the reference of an IKE peer.

Note that this command applies to only IKE negotiation mode.

Related command: **ipsec policy-template**.

Example # Configure a reference to an IKE peer in an IPSec policy.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 isakmp
[Sysname-ipsec-policy-isakmp-policy1-10] ike-peer peer1
```

ipsec binding policy

Syntax **ipsec binding policy** *policy-name* [*seq-number*] [**primary**]

undo ipsec binding policy *policy-name* [*seq-number*] [**primary**]

View Encryption card interface view

Parameter *policy-name*: Name of the IPSec policy, a case insensitive string of 1 to 15 characters. Valid characters are English letters and numbers. No minus sign "-" can be included.

seq-number: Sequence number of the IPSec policy, in the range of 1 to 10000, with a smaller value indicating a higher priority.

primary: Specifies the current encryption card as the primary card of the IPSec policy.

Description Use the **ipsec binding policy** command to bind an IPSec policy or an IPSec policy group to the encryption card interface.

Use the **undo ipsec binding policy** command to remove the binding.

By default, an encryption card interface is bound with no IPSec policy.

Note that:

- An IPSec policy group can be bound to an encryption card either before or after it is applied to an interface as long as you create it first. After binding an IPSec policy group to an encryption card, you must apply it to at least one interface so that the flows matching the policy are to be processed with the encryption card.

- An encryption card interface can be bound with multiple IPSec policy groups or IPSec policies, provided that those policies and policy groups have different names. An IPSec policy group or IPSec policy can be bound to multiple encryption cards.
- An IPSec policy template cannot be bound to an encryption card interface, but an IPSec policy originating from an IPSec policy template can.
- You can specify an encryption card as the primary card when binding an IPSec policy or an IPSec policy group to the card, and you can perform this configuration repeated to specify any other card as the primary card for the IPSec policy or policy group. However, only the last one takes effect. When an IPSec policy or policy group is bound to the current encryption card, the IPSec policy or IPSec policy group with the same name bound before will be overlaid.
- An IPSec policy or policy group uses the bound primary card to provide security services. If there is no primary card, an IPSec policy or policy group prefers the first encryption card bound to it. Once an IPSec policy or policy group takes a second encryption card as the primary card, the new primary card begins to provide security services immediately.

Related command: **ipsec policy (system view)**.

Example # Bind the IPSec policy group named map to interface Encryp1/0.

```
<Sysname> system-view
[Sysname] interface Encrypt 1/0
[Sysname-Encrypt1/0] ipsec binding policy map
```

Bind the IPSec policy with the name of map and sequence number of 10 to interface Encryp1/0.

```
[Sysname] interface Encrypt 1/0
[Sysname-Encrypt1/0] ipsec binding policy map1 10
```

Bind the IPSec policy group named map to Encryp1/0 interface and specify the current encryption card as the primary card.

```
[Sysname] interface Encrypt 1/0
[Sysname-Encrypt1/0] ipsec binding policy map primary
```

Bind the IPSec policy group with name of map and sequence number of 10 to interface Encrypt 1/0 and specify the current encryption card as the primary card.

```
[Sysname] interface Encrypt 1/0
[Sysname-Encrypt1/0] ipsec binding policy map1 10 primary
```

ipsec cpu-backup

Syntax **ipsec cpu-backup enable**

undo ipsec cpu-backup enable

View System view

Parameter None

Description Use the **ipsec cpu-backup enable** command to enable the IPSec module backup function.

Use the **undo ipsec cpu-backup enable** command to disable the IPSec CPU backup function.

By default, the IPSec module backup function is disabled.

Example # Enable the IPSec module backup function.

```
<Sysname> system-view
[Sysname] ipsec cpu-backup enable
```

ipsec policy (interface view)

Syntax **ipsec policy** *policy-name*

undo ipsec policy [*policy-name*]

View Interface view

Parameter *policy-name*: Name of the existing IPSec policy group to be applied to the interface, a string of 1 to 15 characters.

Description Use the **ipsec policy** command to apply an IPSec policy group to an interface.

Use the **undo ipsec policy** command to remove the application of an IPSec policy group.

Note that:

- Only one IPSec policy group can be applied to an interface. To apply another IPSec policy group to the interface, you need to remove the original application and then apply the new one to the interface. An IPSec policy group can be applied to more than one interface.
- With an IPSec policy group applied to an interface, the system uses each IPSec policy in the group to protect certain data flows.
- For each packet to be sent out an IPSec protected interface, the system checks the IPSec policies of the IPSec policy group in the ascending order of sequence numbers. If it finds an IPSec policy whose ACL matches the packet, it uses the IPSec policy to protect the packet. If it finds no ACL of the IPSec policies matches the packet, it does not provide IPSec protection for the packet and sends the packet out directly.

Related command: **ipsec policy (system view)**.

Example # Apply IPSec policy group pg1 to interface Serial 2/2.

```
<Sysname> system-view
[Sysname] interface serial 2/2
[Sysname-Serial2/2] ipsec policy pg1
```

ipsec policy (system view)

Syntax **ipsec policy** *policy-name seq-number* [**isakmp** | **manual**]

undo ipsec policy *policy-name* [*seq-number*]

View System view

Parameter *policy-name*: Name for the IPSec policy, a case insensitive string of 1 to 15 characters. Valid characters are English letters and numbers. No minus sign (-) can be included.

seq-number: Sequence number for the IPSec policy, in the range 1 to 10000.

isakmp: Sets up SAs through IKE negotiation.

manual: Sets up SAs manually.

Description Use the **ipsec policy** command to create an IPSec policy and enter its view.

Use the **undo ipsec policy** command to delete the specified IPSec policies.

By default, no IPSec policy exists.

Note that:

- When creating an IPSec policy, the generation mode will be manual if you do not specify it.
- You cannot change the generation mode of an existing IPSec policy; you can only delete the policy and then re-create it with the new mode.
- IPSec policies with the same name constitute an IPsec policy group. An IPSec policy is identified uniquely by its name and sequence number. In an IPSec policy group, an IPSec policy with a smaller sequence number has a higher priority.
- Using the **undo ipsec policy** command without the *seq-number* argument deletes an IPSec policy group.

Related command: **ipsec policy (interface view)**, **display ipsec policy**.

Example # Create an IPSec policy with the name policy1 and sequence number 100.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100]
```

ipsec policy isakmp template

Syntax **ipsec policy** *policy-name seq-number* **isakmp template** *template-name*

undo ipsec policy *policy-name* [*seq-number*]

View System view

Parameter *policy-name*: Name for the IPSec policy, a case insensitive string of 1 to 15 characters. Valid characters are English letters and numbers. No minus sign (-) can be included.

seq-number: Sequence number for the IPSec policy, in the range 1 to 10000.

template-name: Name for the IPSec policy template to be referenced.

Description Use the **ipsec policy isakmp template** command to create an IPSec policy by referencing an existing IPSec policy template, so that IKE can use IPSec policy for SA negotiation.

Use the **undo ipsec policy** command to delete an IPSec policy.

Note that:

- Using the **undo IPSec policy** command without the *seq-number* argument deletes an IPSec policy group.
- In an IPSec policy, an IPSec policy with a smaller sequence number has a higher priority.

Related command: **ipsec policy (system view)**, **ipsec policy-template**.

Example # Create an IPSec policy with the name *policy2* and sequence number *200* by referencing IPSec policy template temp1.

```
<Sysname> system-view
[Sysname] ipsec policy policy2 200 isakmp template temp1
```

ipsec policy-template

Syntax **ipsec policy-template** *template-name seq-number*

undo ipsec policy-template *template-name* [*seq-number*]

View System view

Parameter *template-name*: Name for the IPSec policy template, a case insensitive string of 1 to 15 characters. Valid characters are English letters and numbers. No minus signs (-) can be included.

seq-number: Sequence number for the IPSec policy template, in the range 1 to 10000.

Description Use the **ipsec policy-template** command to create an IPSec policy template and enter the IPSec policy template view.

Use the **undo ipsec policy-template** command to delete the specified IPSec policy template(s).

By default, no IPSec policy template exists.

Note that:

- Using the **undo** command without the *seq-number* argument deletes an IPSec policy template group.
- In an IPSec policy template group, an IPSec policy template with a smaller sequence number has a higher priority.

Related command: **display ipsec policy-template**.

Example # Create an IPSec policy template with the name *template1* and the sequence number *100*.

```
<Sysname> system-view
[Sysname] ipsec policy-template template1 100
[Sysname-ipsec-policy-template-template1-100]
```

ipsec proposal

Syntax **ipsec proposal** *proposal-name*

undo ipsec proposal *proposal-name*

View System view

Parameter *proposal-name*: Name for the proposal, a case insensitive string of 1 to 15 characters.

Description Use the **ipsec proposal** command to create an IPSec proposal and enter its view.

Use the **undo ipsec proposal** command to delete an IPSec proposal.

By default, no IPSec proposal exists.

Note that an IPSec proposal created by using the **ipsec proposal** command takes the security protocol of ESP, the encryption algorithm of DES, and the authentication algorithm of MD5 by default.

Related command: **display ipsec proposal**.

Example # Create an IPSec proposal named newprop1.

```
<Sysname> system-view
[Sysname] ipsec proposal newprop1
```

ipsec sa global-duration

Syntax **ipsec sa global-duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo ipsec sa global-duration { **time-based** | **traffic-based** }

View System view

Parameter *seconds*: Time-based global SA lifetime in seconds, in the range 180 to 604,800.

kilobytes: Traffic-based global SA lifetime in kilobytes, in the range 256 to 4,194,303.

Description Use the **ipsec sa global-duration** command to configure the global SA lifetime.

Use the **undo ipsec sa global-duration** command to restore the default.

By default, the time-based global SA lifetime is 3,600 seconds, and the traffic-based global SA lifetime is 1,843,200 kilobytes.

Note that:

- When negotiating to set up an SA, IKE prefers the lifetime of the IPSec policy that it uses. If the IPSec policy is not configured with its own lifetime, IKE uses the global SA lifetime.
- When negotiating to set up an SA, IKE prefers the shorter one of the local lifetime and that proposed by the remote.
- The SA lifetime applies to only IKE negotiated SAs; it takes no effect on manually configured SAs.

Related command: **sa duration**, **display ipsec sa duration**.

Example # Set the time-based global SA lifetime to 2 hours, that is, 7,200 seconds.

```
<Sysname> system-view
[Sysname] ipsec sa global-duration time-based 7200
```

Set the traffic-based global SA lifetime to 10M bytes, that is, 10,240 kilobytes.

```
[Sysname] ipsec sa global-duration traffic-based 10240
```

ipsec session idle-time

Syntax **ipsec session idle-time** *seconds*

undo ipsec session idle-time

View System view

Parameter *Seconds*: IPSec session idle timeout in seconds, in the range of 60 to 3,600.

Description Use the **ipsec session idle-time** command to set the idle timeout for IPSec sessions.

Use the **undo ipsec session idle-time** command to restore the default.

By default, the IPSec session idle timeout is 300 seconds.

Example # Set the IPSec session idle timeout to 600 seconds.

```
<Sysname> system-view
[Sysname] ipsec session idle-time 600
```

pfs

Syntax **pfs** { **dh-group1** | **dh-group2** | **dh-group5** | **dh-group14** }

undo pfs

View IPSec policy view/IPSec policy template view

Parameter **dh-group1**: Uses 768-bit Diffie-Hellman group.

dh-group2: Uses 1024-bit Diffie-Hellman group.

dh-group5: Uses 1536-bit Diffie-Hellman group.

dh-group14: Uses 2048-bit Diffie-Hellman group.

Description Use the **pfs** command to enable and configure the perfect forward secrecy (PFS) feature so that the system uses the feature when employing the IPSec policy to initiate a negotiation.

Use the **undo pfs** command to remove the configuration.

By default, the PFS feature is not used for negotiation.

Note that:

- In terms of security and necessary calculation time, the following four groups are in the descending order: 2048-bit Diffie-Hellman group (**dh-group14**), 1536-bit Diffie-Hellman group (**dh-group5**), 1024-bit Diffie-Hellman group (**dh-group2**) and 768-bit Diffie-Hellman group (**group1**).
- This command allows IPSec to perform an additional key exchange process during the negotiation phase 2, providing an additional level of security.

- The local Diffie-Hellman group must be the same as that of the peer.
- This command can be used only when the SAs are to be set up through IKE negotiation.

Related command: **ipsec policy-template**, **ipsec policy (system view)**.

Example # Enable and configure PFS for IPSec policy *policy1*.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 200 isakmp
[Sysname-ipsec-policy-isakmp-policy1-200] pfs dh-group1
```

proposal

Syntax **proposal** *proposal-name*&<1-6>

undo proposal [*proposal-name*]

View IPSec policy view/IPSec policy template view

Parameter *proposal-name*&<1-6>: Name of the IPSec proposal for the IPSec policy to reference, a string of 1 to 15 characters. &<1-6> means that you can specify the *proposal-name* argument for up to six times.

Description Use the **proposal** command to specify the IPSec proposal(s) for the IPSec policy to reference.

Use the **undo proposal** command to remove an IPSec proposal reference by the IPSec policy.

By default, an IPSec policy references no IPSec proposal.

Note that:

- You can specify only existing IPSec proposals when using this command.
- A manual IPSec policy can reference only one IPSec proposal. To replace a referenced IPSec proposal, use the **undo proposal** command to remove the original proposal binding and then use the **proposal** command to reconfigure one.
- An IKE negotiated IPSec policy can reference up to six IPSec proposals. The IKE negotiation process will search for and use the exactly matched proposal.

Related command: **ipsec proposal**, **ipsec policy (system view)**.

Example # Configure IPSec policy policy1 to reference IPSec proposal prop1.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] quit
```

```
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] proposal prop1
```

reset encrypt-card fast-switch

Syntax **reset encrypt-card fast-switch**

View User view

Parameter None

Description Use the **reset encrypt-card fast-switch** command to clear encryption card fast switching entries.

Note that:

- This command clears all the fast switching entries. All IP fast switching entries using the encryption card interface as the inbound interface or outbound interface will also be cleared.
- Once cleared by this command, the fast switching entries cannot be restored.
- Some other actions or events can also clear encryption card fast switching entries, such as disabling the encryption card, resetting the encryption card, hot plugging the encryption card, unbinding a policy and clearing the SA.

Related command: **display encrypt-card fast-switch**.

Example # Clear all encryption card fast switching entries.

```
<sysname> reset encrypt-card fast-switch
```

reset ipsec sa

Syntax **reset ipsec sa** [**parameters** *dest-address protocol spi* | **policy** *policy-name* [*seq-number*] | **remote** *ip-address*]

View User view

Parameter **parameters** *dest-address protocol spi*: Specifies the destination address, security protocol and SPI (Security Parameter Index) of an SA.

dest-address: Destination address in dotted decimal notation.

protocol: Security protocol, which can be keyword **ah** or **esp**, case insensitive.

spi: Security parameter index in the range 256 to 4294967295.

policy: Specifies an IPSec policy.

policy-name: Name of the IPSec policy, a case sensitive string of 1 to 15 alphanumeric characters.

seq-number: Sequence number of the IPSec policy, in the range 1 to 10000. If no *seq-number* is specified, all the policies in the IPSec policy group named *policy-name* are specified.

remote *ip-address*: Specifies *ip-address* as the remote address, in dotted decimal notation.

Description Use the **reset ipsec sa** command to clear an specified or all SAs set up manually or through IKE negotiation.

If no parameter is specified, all SAs will be cleared.

Note that:

- Once an SA set up manually is cleared, the system will automatically set up a new SA based on the parameters of the IPSec policy.
- Once an SA set up through IKE negotiation is cleared, the system will set up a new one through negotiation when a packet triggers an IKE negotiation.
- As SAs appear in pairs, if you specify the **parameters** keyword to clear the SA in one direction, the SA in the other direction will also be cleared.

Related command: **display ipsec sa**.

Example # Clear all SAs.

```
<Sysname> reset ipsec sa
```

Clear the SA with the remote IP address of 10.1.1.2.

```
<Sysname> reset ipsec sa remote 10.1.1.2
```

Clear all SAs of IPSec policy template policy1.

```
<Sysname> reset ipsec sa policy policy1
```

Clear the SA of the IPSec policy with the name of policy1 and sequence number of 10.

```
<Sysname> reset ipsec sa policy policy1 10
```

Clear the SA with the remote IP address of 10.1.1.2, security protocol of AH, and SPI of 10000.

```
<Sysname> reset ipsec sa parameters 10.1.1.2 ah 10000
```

reset ipsec session

Syntax **reset ipsec session** [**tunnel-id** *integer*]

View User view

Parameter *integer*: ID of the IPSec tunnel, in the range1 to 2,000,000,000.

Description Use the **reset ipsec session** command to clear the sessions of a specified or all IPSec tunnels.

Related command: **display ipsec session**.

Example # Clear all IPSec sessions.

```
<Sysname> reset ipsec session
```

Clear the sessions of IPSec tunnel 5.

```
<Sysname> reset ipsec session tunnel-id 5
```

reset ipsec statistics

Syntax **reset ipsec statistics**

View User view

Parameter None

Description Use the **reset ipsec statistics** command to clear IPSec message statistics, and set all the statistics to zero.

Related command: **display ipsec statistics**.

Example # Clear IPSec message statistics.

```
<Sysname> reset ipsec statistics
```

sa authentication-hex

Syntax **sa authentication-hex** { **inbound** | **outbound** } { **ah** | **esp** } *hex-key*

undo sa authentication-hex { **inbound** | **outbound** } { **ah** | **esp** }

View IPSec policy view

Parameter **inbound**: Specifies the inbound SA through which IPSec processes the received packets.

outbound: Specifies the outbound SA through which IPSec process the sent packets.

ah: Uses AH.

esp: Uses ESP.

hex-key: Authentication key for the SA, in hexadecimal format. The length of the key is 16 bytes for MD5 and 20 bytes for SHA1.

Description Use the **sa authentication-hex** command to configure an authentication key for an SA.

Use the **undo sa authentication-hex** command to remove the configuration.

Note that:

- This command applies to only manual IPSec policies.
- When configuring an IPSec policy, you need to set the parameters of both the inbound and outbound SAs.
- The authentication key for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the authentication key for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.
- Both ends of an IPSec tunnel must be configured with the same key in the same format.

Related command: **ipsec policy (system view)**.

Example # Configure the authentication keys of the inbound and outbound SAs using AH as 0x112233445566778899aabbccddeeff00 and 0xaabbccddeeff001100aabbccddeeff00 respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa authentication-hex inbound ah 1
12233445566778899aabbccddeeff00
[Sysname-ipsec-policy-manual-policy1-100] sa authentication-hex outbound ah
aabbccddeeff001100aabbccddeeff00
```

sa duration

Syntax **sa duration** { **time-based** *seconds* | **traffic-based** *kilobytes* }

undo sa duration { **time-based** | **traffic-based** }

View IPSec policy view/IPSec policy template view

Parameter *seconds*: Time-based SA lifetime in seconds, in the range 180 to 604,800.

kilobytes: Traffic-based SA lifetime in kilobytes, in the range 256 to 4,194,303,.

Description Use the **sa duration** command to set an SA lifetime for the IPSec policy.

Use the **undo sa duration** command to restore the default.

By default, the time-based global SA lifetime is 3,600 seconds, and traffic-based SA lifetime is 1,843,200 kilobytes.

Note that:

- When negotiating to set up an SA, IKE prefers the lifetime of the IPSec policy that it uses. If the IPSec policy is not configured with its lifetime, IKE uses the global SA lifetime.
- When negotiating to set up an SA, IKE prefers the shorter one of the local lifetime and that proposed by the remote.
- The SA lifetime applies to only IKE negotiated SAs; it takes no effect on manually configured SAs.

Related command: **ipsec sa global-duration**, **ipsec policy (system view)**.

Example # Set the SA lifetime for the IPSec policy to 2 hours, that is, 7,200 seconds.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration time-based 7200
```

Set the SA lifetime for the IPSec policy to 20 Mbytes, that is, 20,480 kilobytes.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 isakmp
[Sysname-ipsec-policy-isakmp-policy1-100] sa duration traffic-based 20480
```

sa encryption-hex

Syntax **sa encryption-hex** { **inbound** | **outbound** } **esp** *hex-key*

undo sa encryption-hex { **inbound** | **outbound** } **esp**

View IPSec policy view

Parameter **inbound**: Specifies the inbound SA through which IPSec processes the received packets.

outbound: Specifies the outbound SA through which IPSec process the sent packets.

esp: Uses ESP.

hex-key: Encryption key for the SA, in hexadecimal format. The length of the key is 8 bytes for DES and 24 bytes for 3DES.

Description Use the **sa encryption-hex** command to configure an encryption key for an SA.

Use the **undo sa encryption-hex** command to remove the configuration.

Note that:

- This command applies to only manual IPSec policies.
- When configuring an IPSec policy, you need to set the parameters of both the inbound and outbound SAs.
- The encryption key for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the encryption key for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.

Related command: **ipsec policy (system view)**.

Example # Configure the encryption key for the inbound and outbound SAs using ESP as 0x1234567890abcdef and 0xabcdefabcdef1234 respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa encryption-hex inbound
esp 1234567890abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa encryption-hex outbound
 esp abcdefabcdef1234
```

sa spi

Syntax **sa spi** { **inbound** | **outbound** } { **ah** | **esp** } *spi-number*

undo sa spi { **inbound** | **outbound** } { **ah** | **esp** }

View IPSec policy view

Parameter **inbound**: Specifies the inbound SA through which IPSec processes the received packets.

outbound: Specifies the outbound SA through which IPSec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

spi-number: Security parameters index (SPI) in the SA triplet, in the range 256 to 4294967295.

Description Use the **sa spi** command to set the SPI for SA.

Use the **undo sa spi** command to remove the configuration.

Note that:

- This command applies to only manual IPSec policies.

- SA parameters of IKE negotiated IPSec policies are subject to IKE, which is also responsible for establishing SAs.
- When configuring an IPSec policy, you need to set the parameters of both the inbound and outbound SAs.
- The SPI for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the SPI for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.

Related command: **ipsec policy (system view)**.

Example # Configure the SPI of the inbound SA to 10,000 and that of the outbound SA to 20,000.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa spi inbound ah 10000
[Sysname-ipsec-policy-manual-policy1-100] sa spi outbound ah 20000
```

sa string-key

Syntax **sa string-key** { **inbound** | **outbound** } { **ah** | **esp** } *string-key*

undo sa string-key { **inbound** | **outbound** } { **ah** | **esp** }

View IPSec policy view

Parameter **inbound**: Specifies the inbound SA through which. IPSec processes the received packets.

outbound: Specifies the outbound SA through which IPSec processes the packets to be sent.

ah: Uses AH.

esp: Uses ESP.

string-key: Key string for the SA, consisting of 1 to 255 characters. For different algorithms, you can input strings at any length in the specified range. Using this key string, the system automatically generates keys meeting the algorithm requirements. When the protocol is ESP, the system generates the keys for the authentication algorithm and encryption algorithm respectively.

Description Use the **sa string-key** command to set an authentication key for an SA.

Use the **undo sa string-key** command to remove the configuration.

Note that:

- This command applies to only manual IPSec policies.

- When configuring an IPSec policy, you need to set the parameters of both the inbound and outbound SAs.
- The key for the inbound SA at the local end must be the same as that for the outbound SA at the remote end, and the key for the outbound SA at the local end must be the same as that for the inbound SA at the remote end.
- Both ends of an IPSec tunnel must be configured with the same key in the same format.

Related command: **ipsec policy (system view)**.

Example # Configure the keys for the inbound and outbound SAs using AH to abcdef and efcdab respectively.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah abcdef
[Sysname-ipsec-policy-manual-policy1-100] sa string-key inbound ah efcdab
```

security acl

Syntax **security acl** *acl-number*

undo security acl

View IPSec policy view/IPSec policy template view

Parameter *acl-number*: Number of the ACL for the IPSec policy to reference, in the range 3000 to 3999.

Description Use the **security acl** command to specify the ACL for the IPSec policy to reference.

Use the **undo security acl** command to remove the configuration.

By default, an IPSec policy references no ACL.

Related command: **ipsec policy (system view)**.

Example # Configure IPSec policy policy1 to reference ACL 3001.

```
<Sysname> system-view
[Sysname] acl number 3001
[Sysname-acl-adv-3001] rule permit tcp source 10.1.1.0 0.0.0.255 des
tination 10.1.2.0 0.0.0.255
[Sysname-acl-adv-3001] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] security acl 3001
```

transform

Syntax **transform** { **ah** | **ah-esp** | **esp** }

undo transform

View IPSec proposal view

Parameter **ah**: Uses the AH protocol.

ah-esp: Uses ESP first and then AH.

esp: Uses the ESP protocol.

Description Use the **transform** command to specify the security protocol for an IPSec proposal.

Use the **undo transform** command to restore the default.

By default, the ESP protocol is used.

Note that:

- If ESP is used, the default encryption and authentication algorithms are DES and MD5 respectively.
- If AH is used, the default authentication algorithm is MD5.
- If both AH and ESP are used, AH takes the authentication algorithm of MD5 by default, while ESP takes the encryption algorithm of DES and uses no authentication algorithm by default.
- The IPSec proposals at the two ends of an IPSec tunnel must use the same security protocol.

Related command: **ipsec proposal**.

Example # Configure IPSec proposal prop1 to use AH.

```
<Sysname> system-view
[Sysname] ipsec proposal prop1
[Sysname-ipsec-proposal-prop1] transform ah
```

tunnel local

Syntax **tunnel local** *ip-address*

undo tunnel local

View IPSec policy view

Parameter *ip-address*: Local address for the IPSec tunnel.

Description Use the **tunnel local** command to configure the local address of an IPSec tunnel.

Use the **undo tunnel local** command to remove the configuration.

By default, no local address is configured for an IPSec tunnel.

Note that:

- This command applies to only manual IPSec policies.
- The local address, if not configured, will be the address of the interface to which the IPSec policy is applied.

Related command: **ipsec policy (system view)**.

Example # Set the local address of the IPSec tunnel to the address of Loopback0, namely 10.0.0.1.

```
<Sysname> system-view
[Sysname] interface loopback 0
[Sysname-LoopBack0] ip address 10.0.0.1 32
[Sysname-LoopBack0] quit
[Sysname] ipsec policy policy1 100 manual
[Sysname-ipsec-policy-manual-policy1-100] tunnel local 10.0.0.1
```

tunnel remote

Syntax **tunnel remote** *ip-address*

undo tunnel remote [*ip-address*]

View IPSec policy view

Parameter *ip-address*: Remote address for the IPSec tunnel.

Description Use the **tunnel remote** command to configure the remote address of an IPSec tunnel.

Use the **undo tunnel remote** command to remove the configuration.

By default, no remote address is configured for the IPSec tunnel.

Note that:

- This command applies to only manual IPSec policies.
- If you configure the remote address repeatedly, the last one takes effect.
- An IPSec tunnel is established between the local and remote ends. The remote IP address of the local end must be the same as that of the local IP address of the remote end.

Related command: **ipsec policy (system view)**.

Example # Set the remote address of the IPSec tunnel to 10.1.1.2.

```
<Sysname> system-view
[Sysname] ipsec policy policy1 10 manual
[Sysname-ipsec-policy-policy1-10] tunnel remote 10.1.1.2
```

141
IKE CONFIGURATION COMMANDS

authentication-algorithm

Syntax **authentication-algorithm** { **md5** | **sha** }

undo authentication-algorithm

View IKE proposal view

Parameter **md5**: Uses HMAC-MD5.

sha: Uses HMAC-SHA1.

Description Use the **authentication-algorithm** command to specify the authentication algorithm for an IKE proposal.

Use the **undo authentication-algorithm** command to restore the default.

By default, an IKE proposal uses the SHA1 authentication algorithm.

Related command: **ike proposal**, **display ike proposal**.

Example # Set MD5 as the authentication algorithm for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-algorithm md5
```

authentication-method

Syntax **authentication-method** { **pre-share** | **rsa-signature** }

undo authentication-method

View IKE proposal view

Parameter **pre-share**: Uses the pre-shared key method.

rsa-signature: Uses the RSA digital signature method.

Description Use the **authentication-method** command to specify the authentication method to be used by an IKE proposal.

Use the **undo authentication-method** command to restore the default.

By default, an IKE proposal uses the pre-shared key authentication method.

Related command: **ike proposal**, **display ike proposal**.

Example # Specify that IKE proposal 10 uses the pre-shared key authentication method.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] authentication-method pre-share
```

certificate domain

Syntax **certificate domain** *domain-name*

undo certificate domain

View IKE Peer view

Parameter *domain-name*: Name of the PKI domain, a string of 1 to 15 characters.

Description Use the **certificate domain** command to configure the PKI domain of the certificate when IKE uses digital signature as the authentication mode.

Use the **undo certificate domain** command to remove the configuration.

Related command: **authentication-method** on page 1721 and **pki domain** on page 2058.

Example # Configure the PKI domain as abcde for IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer
[Sysname-ike-peer-peer] certificate domain abcde
```

dh

Syntax **dh** { **group1** | **group2** | **group5** | **group14** }

undo dh

View IKE proposal view

Parameter **group1**: Uses the 768-bit Diffie-Hellman group for key negotiation in phase 1.

group2: Uses the 1024-bit Diffie-Hellman group for key negotiation in phase 1.

group5: Uses the 1536-bit Diffie-Hellman group for key negotiation in phase 1.

group14: Uses the 2048-bit Diffie-Hellman group for key negotiation in phase 1.

Description Use the **dh** command to specify the DH group to be used in key negotiation phase 1 for an IKE proposal.

Use the **undo dh** command to restore the default.

By default, group1, the 768-bit Diffie-Hellman group, is used.

Related command: **ike proposal**, **display ike proposal**.

Example # Specify 768-bit Diffie-Hellman for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] dh group1
```

display ike dpd

Syntax **display ike dpd** [*dpd-name*]

View Any view

Parameter *dpd-name*: DPD name, a string of 1 to 15 characters.

Description Use the **display ike dpd** command to display information about a specified or all DPDs.

Related command: **ike dpd**.

Example # Display information about all DPDs.

```
<Sysname> display ike dpd

---------------------------
 IKE dpd: dpd1
   references: 1
   interval-time: 10
   time_out: 5
---------------------------
```

Table 569 Description on the fields of the display ike dpd command

Field	Description
references	Number of IKE peers referencing the DPD
Interval-time	DPD query triggering interval in seconds
time_out	DPD packet retransmission interval in seconds

display ike peer

Syntax **display ike peer** [*peer-name*]

View Any view

Parameter *peer-name*: Name of the IKE peer, a string of 1 to 15 characters.

Description Use the **display ike peer** command to display information about a specified or all IKE peers.

Related command: **ike peer (system view)**.

Example # Display information about all IKE peers.

```
<Sysname> display ike peer

---------------------------
 IKE Peer: rtb4tunn
   exchange mode: main on phase 1
   pre-shared-key: 123
   peer id type: ip
   peer ip address: 44.44.44.55
   local ip address:
   peer name:
   nat traversal: disable
   dpd: dpd1
---------------------------
```

Table 570 Description on the fields of the display ike peer command

Field	Description
exchange mode	IKE negotiation mode in phase 1
pre-shared-key	Pre-shared key used in phase 1
peer id type	ID type used in phase 1
peer ip address	IP address of the remote security gateway
local ip address	IP address of the local security gateway
peer name	Name of the remote security gateway
nat traversal	Whether NAT traversal is enabled
dpd	Name of the peer DPD

display ike proposal

Syntax **display ike proposal**

View Any view

Parameter None

Description Use the **display ike proposal** command to display the settings of all IKE proposals.

This command displays the configuration information of all IKE proposals in the descending order of proposal priorities.

Related command: **authentication-method** on page 1721, **ike proposal**, **encryption-algorithm** on page 1725, **authentication-algorithm** on page 1721, **dh**, **sa duration**.

Example # Display the settings of IKE proposals.

```
<Sysname> display ike proposal
priority authentication authentication encryption Diffie-Hellman duration
              method       algorithm    algorithm     group       (seconds)
------------------------------------------------------------------------------
 10       PRE_SHARED     SHA            DES_CBC    MODP_1024      5000
 11       PRE_SHARED     MD5            DES_CBC    MODP_768       50000
 default  PRE_SHARED     SHA            DES_CBC    MODP_768       86400
```

Table 571 Description on the fields of the display ike proposal command

Field	Description
priority	Priority of the IKE proposal
authentication method	Authentication method used by the IKE proposal
authentication algorithm	Authentication algorithm used by the IKE proposal
encryption algorithm	Encryption algorithm used by the IKE proposal
Diffie-Hellman group	DH group used in IKE negotiation in phase 1
duration (seconds)	ISAKMP SA lifetime of the IKE proposal in seconds

display ike sa

Syntax **display ike sa [verbose [connection-id** *connection-id* | **remote-address** *remote-address*]]

View Any view

Parameter **verbose**: Displays detailed information.

connection-id: Displays detailed information about IKE SAs by connection ID, in the range 1 to 2000000000.

remote-address: Displays detailed information about IKE SAs by remote address.

Description Use the **display ike sa** command to display information about the current IKE SAs.

Note that the command displays brief information about the current IKE SAs if you specify no parameters or keywords.

Related command: **ike proposal**, **ike peer (system view)**.

Example # Display brief information about the current IKE SAs.

```
<Sysname> display ike sa
    total phase-1 SAs:  1
    connection-id  peer            flag        phase   doi
  -----------------------------------------------------------
      1            202.38.0.2      RD|ST        1      IPSEC
      2            202.38.0.2      RD|ST        2      IPSEC
flag meaning
RD--READY ST--STAYALIVE RL--REPLACED FD-FADING TO--TIMEOUT
```

Table 572 Description on the fields of the display ike sa command

Field	Description
total phase-1 SAs	Total number of SAs in phase 1
connection-id	Identifier of the IPSec tunnel
peer	Remote IP address of the SA
flag	Status of the SA: ■ RD (READY): the SA has been established. ■ ST (STAYALIVE): This end is the initiator of the tunnel negotiation. ■ RL (REPLACED): The tunnel has been replaced by a new one and will be deleted later. ■ FD (FADING): The tunnel is soft timed out but still in use. It will be deleted when it is hard timed out. ■ TO (TIMEOUT): The SA has received no keepalive packets after the last keepalive timeout. If no keepalive packets are received before the next keepalive timeout, the SA will be deleted.
phase	The phase the SA belongs to: ■ Phase 1: The phase for establishing the ISAKMP SA. ■ Phase 2: The phase for negotiating the security service. IPSec SAs are established in this phase.
doi	Domain of interpretation the SA belongs to

Display detailed information about the current IKE SAs.

```
<Sysname>display ike sa verbose
    -------------------------------------------
    connection id: 2
    transmitting entity: initiator
    -------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 86379
    exchange-mode: MAIN
```

```
    diffie-hellman group: GROUP1
    nat traversal: NO
```

Display detailed information about the IKE SA with the connection ID of 2.

```
<Sysname>display ike sa verbose connection-id 2
    -----------------------------------------------
    connection id: 2
    transmitting entity: initiator
    -----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82480
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

Display detailed information about the IKE SA with the remote address of 4.4.4.5..

```
<Sysname>display ike sa verbose remote-address 4.4.4.5
    -----------------------------------------------
    connection id: 2
    transmitting entity: initiator
    -----------------------------------------------
    local ip: 4.4.4.4
    local id type: IPV4_ADDR
    local id: 4.4.4.4

    remote ip: 4.4.4.5
    remote id type: IPV4_ADDR
    remote id: 4.4.4.5

    authentication-method: PRE-SHARED-KEY
    authentication-algorithm: HASH-SHA1
    encryption-algorithm: DES-CBC

    life duration(sec): 86400
    remaining key duration(sec): 82236
    exchange-mode: MAIN
    diffie-hellman group: GROUP1
    nat traversal: NO
```

dpd

Syntax **dpd** *dpd-name*

undo dpd

View IKE Peer view

Parameter *dpd-name*: DPD name, a string of 1 to 15 characters.

Description Use the **dpd** command to apply a DPD to an IKE peer.

Use the **undo dpd** command to remove the application.

By default, no DPD is applied to an IKE peer.

Example # Apply DPD dpd1 to IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] dpd dpd1
```

encryption-algorithm

Syntax **encryption-algorithm** { **3des-cbc** | **aes-cbc** [*key-length*] | **des-cbc** }

undo encryption-algorithm

View IKE proposal view

Parameter **3des-cbc**: Uses the 3DES algorithm in CBC mode as the encryption algorithm. The 3DES algorithm uses 168-bit keys for encryption.

aes-cbc: Uses the AES algorithm in CBC mode as the encryption algorithm. The AES algorithm uses 128-bit, 192-bit, or 256-bit keys for encryption.

key-length: Key length for the AES algorithm, which can be 128, 192 or 256 bits and is defaulted to 128 bits.

des-cbc: Uses the DES algorithm in CBC mode as the encryption algorithm. The DES algorithm uses 56-bit keys for encryption.

Description Use the **encryption-algorithm** command to specify the encryption algorithm for an IKE proposal.

Use the **undo encryption-algorithm** command to restore the default.

By default, an IKE proposal uses the 56-bit DES encryption algorithm in CBC mode.

Related command: **ike proposal** and **display ike proposal**.

Example # Use 56-bit DES in CBC mode as the encryption algorithm for IKE proposal 10.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] encryption-algorithm des-cbc
```

exchange-mode

Syntax **exchange-mode** { **aggressive** | **main** }

undo exchange-mode

View IKE Peer view

Parameter **aggressive**: Aggressive mode

main: Main mode.

Description Use the **exchange-mode** command to select an IKE negotiation mode.

Use the **undo exchange-mode** command to restore the default.

By default, main mode is used.

Note that if the user at one end of an IPSec tunnel obtains IP address automatically (for example, a dial-up user), IKE negotiation mode must be set to **aggressive**. In this case, an SA can be created as long as the username and password are correct.

Related command: **id-type**.

Example # Specify that IKE negotiation works in main mode.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] exchange-mode main
```

id-type

Syntax **id-type** { **ip** | **name** }

undo id-type

View IKE Peer view

Parameter **ip**: Uses an IP address as the ID in IKE negotiation.

name: Uses a name as the ID in IKE negotiation.

Description Use the **id-type** command to select the type of the ID in IKE negotiation.

Use the **undo id-type** command to restore the default.

By default, the type of IP address is used in IKE negotiation.

Note that:

- In main mode, only the ID type of IP address can be used in performing IKE negotiation and creating an SA.
- In aggressive mode, either type can be used.

Related command: **ike local-name**, **remote-name**, **remote-address**, **local-address**, **exchange-mode**.

Example # Use the ID type of name in IKE negotiation.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] id-type name
```

ike dpd

Syntax **ike dpd** *dpd-name*

undo ike dpd *dpd-name*

View System view

Parameter *dpd-name*: Name for the dead peer detection (DPD), a string of 1 to 15 characters.

Description Use the **ike dpd** command to create a DPD and enter IKE DPD view.

Use the **undo ike dpd** command to remove a DPD.

Example # Create a DPD named dpd2.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
```

ike local-name

Syntax **ike local-name** *name*

undo ike local-name

View System view

Parameter *name*: Name of the local gateway for IKE negotiation, a string of 1 to 32 characters.

Description Use the **ike local-name** command to configure a name for the local gateway.

Use the **undo ike local-name** command to restore the default.

By default, the device name is used as the name of the local gateway

If the IKE negotiation initiator uses the gateway name to perform IKE negotiation (that is, the **id-type name** command is configured on the initiator), you need to configure the **ike local-name** command on the local device. The IKE negotiation initiator sends its gateway name as identification to its peer and the peer uses the gateway name configured with the **remote-name** *name* command to authenticate the initiator. Therefore, make sure the local gateway name for a device is identical to the remote gateway name configured on its peer.

Related command: **remote-name**, **id-type name**.

Example # Configure the local gateway name as app.

```
<Sysname> system-view
[Sysname] ike local-name app
```

ike next-payload check disabled

Syntax **ike next-payload check disabled**

undo ike next-payload check disabled

View System view

Parameter None

Description Use the **ike next-payload check disabled** command to disable the checking of the Next payload field in the last payload of an IKE message during IPSec negotiation, gaining interoperation with products assigning the field a value other than zero.

Use the **undo ike next-payload check disabled** command to restore the default.

By default, the Next payload field is checked.

Example # Disable Next payload field checking for the last payload of an IKE message.

```
<Sysname> system-view
[Sysname] ike next-payload check disabled
```

ike peer (system view)

Syntax **ike peer** *peer-name*

undo ike peer *peer-name*

View System view

Parameter *peer-name*: IKE peer name, a string of 1 to 15 characters.

Description Use the **ike peer** command to create an IKE peer and enter IKE peer view.

Use the **undo ike peer** command to delete an IKE peer.

Example # Create an IKE peer named peer1 and enter IKE peer view.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1]
```

ike proposal

Syntax **ike proposal** proposal-number

undo ike proposal *proposal-number*

View System view

Parameter *proposal-number*: IKE proposal number, in the range 1 to 100. It also stands for the priority, with a smaller value meaning a higher priority. During an IKE negotiation, the system matches IKE proposals by proposal number, starting from the smallest one.

Description Use the **ike proposal** command to create an IKE proposal and enter IKE proposal view.

Use the **undo ike proposal** command to delete an IKE proposal.

The system provides a default IKE proposal, which has the lowest priority and uses these settings.

- Encryption algorithm: DES-CBC;
- Authentication algorithm: HMAC-SHA1;
- Authentication method: Pre-shared Key;
- DH group: MODP_768;
- SA lifetime: 86, 400 seconds.

Related command: **display ike proposal**.

Example # Create IKE proposal 10 and enter IKE proposal view.

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10]
```

ike sa keepalive-timer interval

Syntax **ike sa keepalive-timer interval** *seconds*

undo ike sa keepalive-timer interval

View System view

Parameter *seconds*: Transmission interval of ISAKMP SA keepalives in seconds, in the range 20 to 28,800.

Description Use the **ike sa keepalive-timer interval** command to set the ISAKMP SA keepalive interval.

Use the **undo ike sa keepalive-timer interval** command to disable the ISAKMP SA keepalive transmission function.

By default, no keepalive packet is sent.

Note that the keepalive interval configured at the local end must be shorter than the keepalive timeout configured at the remote end.

Related command: **ike sa keepalive-timer timeout**.

Example # Set the keepalive interval to 200 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer interval 200
```

ike sa keepalive-timer timeout

Syntax **ike sa keepalive-timer timeout** *seconds*

undo ike sa keepalive-timer timeout

View System view

Parameter *seconds*: ISAKMP SA keepalive timeout in seconds, in the range 20 to 28,800.

Description Use the **ike sa keepalive-timer timeout** command to asset the ISAKMP SA keepalive timeout.

Use the **undo ike sa keepalive-timer timeout** command to disable the function.

By default, no keepalive packet is sent.

Note that the keepalive timeout configured at the local end must be longer than the keepalive interval configured at the remote end. Since it seldom occurs that more than three consecutive packets are lost on a network, the keepalive timeout can be configured to be three times of the keepalive interval.

Related command: **ike sa keepalive-timer interval**.

Example # Set the keepalive timeout to 20 seconds.

```
<Sysname> system-view
[Sysname] ike sa keepalive-timer timeout 20
```

ike sa nat-keepalive-timer interval

Syntax **ike sa nat-keepalive-timer interval** *seconds*

undo ike sa nat-keepalive-timer interval

View System view

Parameter *seconds*: NAT keepalive interval in seconds, in the range 5 to 300.

Description Use the **ike sa nat-keepalive-timer interval** command to set the NAT keepalive interval.

Use the **undo ike sa nat-keepalive-timer interval** command to disable the function.

By default, no NAT keepalive packet is sent.

Example # Set the NAT keepalive interval to 5 seconds.

```
<Sysname> system-view
[Sysname] ike sa nat-keepalive-timer interval 5
```

interval-time

Syntax **interval-time** *interval-time*

undo interval-time

View IKE DPD view

Parameter *interval-time*: Interval in seconds at which DPD query is triggered if no IPSec packet is received from the peer, in the range 1 to 300.

Description Use the **interval-time** command to set the DPD query triggering interval for a DPD.

Use the **undo interval-time** command to restore the default.

By default, the DPD query triggering interval is 10 seconds.

Example # Set the DPD query triggering interval for dpd2 to 1 second.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] interval-time 1
```

local

Syntax **local** { **multi-subnet** | **single-subnet** }

undo local

View IKE peer view

Parameter **multi-subnet**: Sets the subnet type to multiple.

single-subnet: Sets the subnet type to single.

Description Use the **local** command to set the subnet type of the local gateway for IKE negotiation.

Use the **undo local** command to restore the default.

By default, the subnet is a single one. You can use this command to enable interoperability with a Netscreen device.

Example # Set the subnet type of the local gateway to multiple.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local multi-subnet
```

local-address

Syntax **local-address** *ip-address*

undo local-address

View IKE peer view

Parameter *ip-address*: IP address of the local gateway in IKE negotiation.

Description Use the **local-address** command to configure the IP address of the local gateway in IKE negotiation.

Use the **undo local-address** command to remove the configuration.

By default, the master address of the interface referencing the IPSec policy is used as the local gateway IP address for IKE negotiation. This command is required only when you want to specify a special address for the local gateway.

Example # Set the IP address of the local gateway to 1.1.1.1.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] local-address 1.1.1.1
```

nat traversal

Syntax **nat traversal**

undo nat traversal

View IKE peer view

Parameter None

Description Use the **nat traversal** command to enable the NAT traversal function of IKE/IPSec.

Use the **undo nat traversal** command to disable the NAT traversal function of IKE/IPSec.

By default, the NAT traversal function is disabled.

Example # Enable the NAT traversal function for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] nat traversal
```

peer

Syntax **peer** { **multi-subnet** | **single-subnet** }

undo peer

View IKE peer view

Parameter **multi-subnet**: Sets the subnet type to multiple.

single-subnet: Sets the subnet type to single.

Description Use the **peer** command to set the subnet type of the peer gateway for IKE negotiation.

Use the **undo peer** command to restore the default.

By default, the subnet is a single one. You can use this command to enable interoperability with a Netscreen device.

Example # Set the subnet type of the peer gateway to multiple.

```
<Sysname> system-view
[Sysname] ike peer xhy
[Sysname-ike-peer-xhy] peer multi-subnet
```

pre-shared-key

Syntax **pre-shared-key** *key*

undo pre-shared-key

View IKE peer view

Parameter *key*: Pre-shared key, a case sensitive string of 1 to 128 characters.

Description Use the **pre-shared-key** command to configure the pre-shared key to be used in IKE negotiation.

Use the **undo pre-shared-key** command to remove the configuration.

Related command: **authentication-algorithm** on page 1721.

Example # Set the pre-shared key used in IKE negotiation to abcde.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] pre-shared-key abcde
```

remote-address

Syntax **remote-address** *low-ip-address* [*high-ip-address*]

undo remote-address

View IKE peer view

Parameter *low-ip-address*: Remote IP address of the IPSec tunnel. It is the lowest address in the address range if you want to specify a range of addresses.

high-ip-address: Highest address in the address range if you want to specify a ragne of addresses.

Description Use the **remote-address** command to configure the remote IP address of the IPSec tunnel.

Use the **undo remote-address** command to remove the configuration.

Note that the *ip-address* configured with the **remote-address** command must agree with the IP address configured with the **local-address** command.

Related command: **id-type ip**, **local-address**.

Example # Configure the remote IP address as 10.0.0.1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-address 10.0.0.1
```

remote-name

Syntax **remote-name** *name*

undo remote-name

View IKE peer view

Parameter *name*: Name of the peer gateway for IKE negotiation, a string of 1 to 32 characters.

Description Use the **remote-name** command to configure the name of the remote gateway.

Use the **undo remote-name** command to remove the configuration.

If the IKE negotiation initiator uses its gateway name for IKE negotiation (that is, the **id-type name** command is configured on the initiator), it sends the name as its identity to the peer, whereas the peer uses the gateway name configured with the **remote-name** *name* command to authenticate the initiator. Therefore, the local gateway name for a device must be identical to the remote gateway name configured on its peer.

Related command: **id-type**, **ike local-name**.

Example # Configure the remote gateway name as apple for IKE peer peer1.

```
<Sysname> system-view
[Sysname] ike peer peer1
[Sysname-ike-peer-peer1] remote-name apple
```

reset ike sa

Syntax **reset ike sa** [*connection-id*]

View User view

Parameter *connection-id*: Connection ID of the IPSec tunnel to be cleared, in the range 1 to 2000000000.

Description Use the **reset ike sa** command to clear the IPSec tunnel set up by IKE.

Note that:

- If *connection-id* is not specified, all the SAs set up in phase 1 will be cleared.
- When clearing the local IPSec tunnel, if there is an ISAKMP SA of phase 1, a Delete Message will be sent to the remote end under the protection of this IPSec tunnel to notify the remote end of deleting the corresponding SA.
- If ISAKMP SAs of phase 1 are cleared first, the remote end cannot be notified to clear the corresponding SAs when you clear the SAs of phase 2.

Related command: **display ike sa**.

Example # Clear the IPSec tunnel to 202.38.0.2.

```
<Sysname> display ike sa
conn-id      remote          flag         phase     doi
1            202.38.0.2      RD|ST        1         IPSEC
2            202.38.0.2      RD|ST        2         IPSEC
flag meaning:
RD--READY ST--STAYALIVE RL--REPLACED FD-FADING TO--TIMEOUT
<Sysname> reset ike sa 2
<Sysname> display ike sa
conn-id      remote        flag           phase      doi
1            202.38.0.2    RD|ST          1          IPSEC
flag meaning:
RD--READY ST--STAYALIVE RL--REPLACED FD-FADING TO-TIMEOUT
```

sa duration

Syntax **sa duration** *seconds*

undo sa duration

View IKE proposal view

Parameter *Seconds*: Specifies the ISAKMP SA lifetime in seconds, in the range 60 to 604800.

Description Use the **sa duration** command to specify the ISAKMP SA lifetime for an IKE proposal.

Use the **undo sa duration** command to restore the default.

By default, the ISAKMP SA lifetime is 86,400 seconds.

Before an SA expires, IKE will negotiate a new SA. As soon as the new SA is set up, it takes effect immediately and the old one will be cleared automatically when it expires.

Related command: **ike proposal** and **display ike proposal**.

Example # Specify the ISAKMP SA lifetime for IKE proposal 10 as 600 seconds (10 minutes).

```
<Sysname> system-view
[Sysname] ike proposal 10
[Sysname-ike-proposal-10] sa duration 600
```

time-out

Syntax **time-out** time-out

undo time-out

View IKE DPD view

Parameter *time-out*: DPD packet retransmission interval in seconds, in the range 1 to 60.

Description Use the **time-out** command to set the DPD packet retransmission interval for a DPD.

Use the **undo time-out** command to restore the default.

By default, the DPD packet retransmission interval is 5 seconds.

Example # Set the DPD packet retransmission interval for dpd2 to 1 second.

```
<Sysname> system-view
[Sysname] ike dpd dpd2
[Sysname-ike-dpd-dpd2] time-out 1
```

142 SSH2.0 CONFIGURATION COMMANDS

display public-key local

Syntax **display public-key local { dsa | rsa } public**

View Any view

Parameter **dsa**: Displays the public key(s) of DSA local key pair(s).

rsa: Displays the public key(s) of RSA local key pair(s).

Description Use the display public-key local command to display information about the public key(s) of the local key pair(s).

Related command: **public-key local create**.

Example # Display the public key information of RSA local key pair(s).

```
<Sysname> display rsa local-key-pair public
=====================================================
Time of Key pair created: 19:59:16  2006/10/25
Key name: HOST_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
30819F300D06092A864886F70D01010105000381 8D003081 8902818100BC4C392A97
734A633BA0F1DB01F84EB51228EC86ADE1DBA597E0D9066FDC4F04776CEA3610D257
8341F5D049143656F1287502C06D39D39F28F0F5CBA630DA8CD1C16ECE8A7A65282F
2407E8757E7937DCCDB5DB620CD1F471401B7117139702348444A2D8900497A87B8D
5F13D61C4DEFA3D14A7DC07624791FC1D226F62DF3020301
0001

=====================================================
Time of Key pair created: 19:59:17  2006/10/25
Key name: SERVER_KEY
Key type: RSA Encryption Key
=====================================================
Key code:
307C300D06092A864886F70D0101010500036B003068026100C51AF7CA926962284A
4654B2AACC7B2AE12B2B1EABFAC1CDA97E42C3C10D7A70D1012BF23ADE5AC4E7AAB1
32CFB6453B27E054BFAA0A85E113FBDE751EE0ECEF659529E857CF8C211E2A03FD8F
10C5BEC162B2989ABB5D299D1E4E27A13C7DD10203010001
```

Display the public key information of DSA local key pair(s).

```
<Sysname> display public-key local dsa public

=====================================================
Time of Key pair created: 20:00:16  2006/10/25
Key name: HOST_KEY
Key type: DSA Encryption Key
=====================================================
Key code:
308201B83082012C06072A8648CE3804013082011F02818100D757262C4584C44C21
1F18BD96E5F061C4F0A423F7FE6B6B85B34CEF72CE14A0D3A5222FE08CECE65BE6C2
65854889DC1EDBD13EC8B274DA9F75BA26CCB987723602787E922BA84421F22C3C89
CB9B06FD60FE01941DDD77FE6B12893DA76EEBC1D128D97F0678D7722B5341C8506F
358214B16A2FAC4B368950387811C7DA33021500C773218C737EC8EE993B4F2DED30
F48EDACE915F02818100822690 09E14EC474BAF2932E69D3B1F18517AD9594184CCD
FCEAE96EC4D5EF93133E84B47093C52B20CD35D02492B3959EC6499625BC4FA5082E
22C5B374E16DD00132CE71B020217091AC717B612391C76C1FB2E88317C1BD8171D4
1ECB83E210C03CC9B32E810561C21621C73D6DAAC028F4B1585DA7F42519718CC9B0
9EEF038185000 2818100CCF1F78E0860BE937FD3CA07D2F2A1B66E74E5D1E16693EB
374D677A7A6124EBABD59FE48796C56F3FF919F999AEB97D1F2B83D9B98AC09BC1F7
2E80DBE337CB29989A23378EB21C38EE083F11ED6DC8D4DBE001BA85450CEA071C2A
471C83761E4CF32C174B418612CDD597B441F0CAA05DC01CB93A0ABB247C06FB
A4C79054
```

Table 573 Description on fields of the display public-key local command

Field	Description
Time of Key pair created	Time when the key pair is created
Key name	Name of the key
Key type	Type of the key
Key code	Code of the key

display public-key peer

Syntax **display public-key peer** [**brief** | **name** *publickey-name*]

View Any view

Parameter **brief**: Displays brief information about all public keys.

name *publickey-name*: Specifies a public key by its name, which is a string of 1 to 64 characters.

Description Use the **display public-key peer** command to display information about a specified or all public keys.

With neither the **brief** keyword nor the **name** *publickey-name* combination specified, the command displays detailed information about all public keys.

Related command: **public-key peer**.

Example # Display detailed information about public key **idrsa**.

```
<Sysname> display public-key peer name idrsa
=====================================
  Key name  : idrsa
  Key type  : RSA
  Key module: 1024
=====================================
Key Code:
30819D300D06092A864886F70D010101050003818B003081870281810090C46A87102
16CEC0C01C7CE136BA76C79AA6040E79F9E305E453998C7ADE8276069410803D5974
F708496947AB39B3F39C5CE56C95B6AB7442D56393BF241F99A639DD02D9E29B1F5C
1FD05CC1C44FBD6CFFB58BE6F035FAA2C596B27D1231D159846B7CB9A7757C5800FA
DA9FD72F65672F4A549EE99F63095E11BD37789955020123
```

Table 574 Description on fields of the display public-key peer command

Field	Description
Key name	Name of the key
Key type	Type of the key
Key module	Module of the key
Key code	Code of the key

Display brief information about all public keys.

```
<Sysname> display public-key peer brief
Type  Module  Name
---------------------------
RSA   1024    idrsa
DSA   1024    10.1.1.1
```

Table 575 Description on the fields of the display public-key peer brief command

Field	Description
Type	Type of the key
Module	Number of bits in the peer public key
Name	Name of the peer public key

display sftp client source

Syntax **display sftp client source**

View Any view

Parameter None

Description Use the **display sftp client source** command to display the source IP address or source interface currently set for the SFTP client.

If neither source IP address nor source interface is specified for the SFTP client, "You didn't specify the source" will be displayed.

Related command: **sftp client source**.

Example # Display the source IP address of the SFTP client.

```
<Sysname> display sftp client source
The source IP address you specified is 192.168.0.1
```

display ssh client source

Syntax **display ssh client source**

View Any view

Parameter None

Description Use the **display ssh client source** command to display the source IP address or source interface currently set for the SSH client.

If neither source IP address nor source interface is specified for the SSH client, "You didn't specify the source" will be displayed.

Related command: **ssh client source**.

Example # Display the source IP address of the SSH client.

```
<Sysname> display ssh client source
The source IP address you specified is 192.168.0.1
```

display ssh server

Syntax **display ssh server** { **status** | **session** }

View Any view

Parameter **status**: Displays the status information of the SSH server.

session: Displays the session information of the SSH server.

Description Use the **display ssh server** command to display the status information or session information of an SSH server.

Related command: **ssh server authentication-retries**, **ssh server rekey-interval**, **ssh server authentication-timeout**, **ssh server enable**, and **ssh server compatible-ssh1x enable**.

Example # Display the status information of the SSH server.

```
<Sysname> display ssh server status
 SSH Server: Disable
 SSH version : 1.99
 SSH authentication-timeout : 60 second(s)
```

```
SSH server key generating interval : 0 hour(s)
SSH Authentication retries : 3 time(s)
SFTP Server: Disable
SFTP Server Idle-Timeout: 10 minute(s)
```

Table 576 Description on fields of the display ssh server status command

Field	Description
SSH Server	Whether the SSH server function is enabled
SSH version	SSH protocol version When the SSH supports SSH1, the protocol version is 1.99. Otherwise, the protocol version is 2.0.
SSH authentication-timeout	Authentication timeout period
SSH server key generating interval	SSH server key pair update interval
SSH Authentication retries	Maximum number of SSH authentication attempts
SFTP Server	Whether the SFTP server function is enabled
SFTP Server Idle-Timeout	SFTP connection idle timeout period

Display the session information of the SSH server.

```
<Sysname> display ssh server session
 Conn    Ver    Encry     State      Retry     SerType  Username
 VTY 0   2.0    DES     Established    0         SFTP     client001
```

Table 577 Description on fields of the display ssh server session command

Field	Description
Conn	Connected VTY channel
Ver	SSH server protocol version
Encry	Encryption algorithm
State	Status of the session, including: Init: initializing Ver-exchange: version exchanging Keys-exchange: keys exchanging Auth-request: user authenticating Serv-request: service requesting Established: connection established Disconnected: connection disconnected
Retry	Number of authentication attempts
SerType	Service type, either SFTP or Stelnet
Username	Name of a user for login

display ssh server-info

Syntax **display ssh server-info**

View Any view

Parameter None

Description Use the **display ssh server-info** command to display the mappings between host public keys and SSH servers saved on a client.

Example # Display the mappings between host public keys and SSH servers saved on the client.

```
<Sysname> display ssh server-info
Server Name(IP)                 Server public key name
_____________________________________________________
192.168.0.1                      abc_key01
192.168.0.2                      abc_key02
```

Table 578 Descriptions on fields of the display ssh server-info command

Field	Description
Server Name(IP)	Name or IP address of the server
Server public key name	Name of the host public key of the server

display ssh user-information

Syntax **display ssh user-information** [*username*]

View Any view

Parameter *username*: SSH username, a string of 1 to 80 characters.

Description Use the **display ssh user-information** command to display information about a specified or all SSH users.

With the *username* argument not specified, the command displays information about all SSH users.

Related command: **ssh user**.

Example # Display information about all SSH users.

```
<Sysname> display ssh user-information
 Total ssh users : 2
Username    Authentication-type   User-public-key-name     Service-type
 yemx        password              putty                    stelnet|sftp
 test        publickey             null                     sftp
```

Table 579 Description on fields of the display ssh user-information command

Field	Description
Username	Name of the user
Authentication-type	Authentication type
User-public-key-name	Public key of the user
Service-type	Service type

peer-public-key end

Syntax **peer-public-key end**

View Public key view

Parameter None

Description Use the **peer-public-key end** command to return from public key view to system view.

Related command: **public-key peer**.

Example # Exit public key view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] peer-public-key end
[Sysname]
```

public-key-code begin

Syntax **public-key-code begin**

View Public key view

Parameter None

Description Use the **public-key-code begin** command to enter RSA key code view.

After entering public key code view, you can input the key data. It must be a hexadecimal string that is generated randomly by the SSH-supported client software and coded compliant to PKCS.

Related command: **public-key peer**, **public-key-code end**.

Example # Enter public key code view to input the key.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D003
0818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308
C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B8
54E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276
FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
```

public-key-code end

Syntax **public-key-code end**

View RSA key code view

Parameter None

Description Use the **public-key-code end** command to return from public key code view to public key view and to save the configured public key.

The system verifies the key before saving it. If the key contains illegal characters, the system displays an error message and discards the key. If the key is legal, the system saves it.

Related command: **public-key peer**, **public-key-code begin**.

Example # Exit RSA key code view.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key] public-key-code begin
[Sysname-pkey-key-code]30819F300D06092A864886F70D010101050003818D003
0818902818100C0EC8014F82515F6335A0A
[Sysname-pkey-key-code]EF8F999C01EC94E5760A079BD73E4F4D97F3500EDB308
C29481B77E719D1643135877E13B1C531B4
[Sysname-pkey-key-code]FF1877A5E2E7B1FA4710DB0744F66F6600EEFE166F1B8
54E2371D5B952ADF6B80EB5F52698FCF3D6
[Sysname-pkey-key-code]1F0C2EAAD9813ECB16C5C7DC09812D4EE3E9A0B074276
FFD4AF2050BD4A9B1DDE675AC30CB020301
[Sysname-pkey-key-code]0001
[Sysname-pkey-key-code] public-key-code end
[Sysname-pkey-public-key]
```

public-key local create

Syntax **public-key local create** { **dsa** | **rsa** }

View System view

Parameter **dsa**: DSA key pair.

rsa: RSA key pair.

Description Use the **public-key local create** command to create the local key pairs.

Note that:

- After entering this command, you will be prompted to provide the length of the key pair. The length of a server/host key must be in the range 512 to 2048

bits and defaults to 1024. If the key pair already exists, the system will ask you whether you want to overwrite it.

- The configuration of this command can survive a reboot. You only need to configure it once.

Related command: **public-key local destroy**, **display public-key local**.

Example # Create local RSA key pair.

```
<Sysname> system-view
[Sysname] public-key local create rsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It may take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus [default = 1024]:
Generating keys...
........++++++
.....................................++++++
.......++++++++
.....................++++++++
.
```

Create local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local create dsa
The range of public key size is (512 ~ 2048).
NOTES: If the key modulus is greater than 512,
       It will take a few minutes.
Press CTRL+C to abort.
Input the bits in the modulus[default = 1024]:
Generating keys...
.+++++++++++++++++++++++++++++++++++++++++++++++++*
........+......+.....+.....................................+..+....
...................+..........+.............+.............+...+....
.+..............+..+......+................+..........+...+....+..
.....+.....+............+.........+.......................+.......
.+..........+.............+.....+...+.......................+.....
....+..........+...........+........+....+.....................+++
++++++++++++++++++++++++++++++++++++++++++++++++*
.
```

- *Pressing **CTRL+C** quits the session of generating the local RSA key pair rather than aborting the generation of the local RSA key pair.*
- *Be sure to press **CTRL+C** before inputting the bits in the modulus.*

public-key local destroy

Syntax **public-key local destroy** { **dsa** | **rsa** }

View System view

Parameter **dsa**: DSA key pair.

rsa: RSA key pair.

Description Use the **public-key local destroy** command to destroy the local key pair(s).

Related command: **public-key local create**.

Example # Destroy local RSA key pair.

```
<Sysname> system-view
[Sysname] public-key local destroy rsa
Warning: Confirm to destroy these keys? [Y/N]:y
```

Destroy local DSA key pair.

```
<Sysname> system-view
[Sysname] public-key local destroy dsa
Warning: Confirm to destroy these keys? [Y/N] : y
```

public-key local export rsa

Syntax **public-key local export rsa** { **openssh** | **ssh1** | **ssh2** } [*filename*]

View System view

Parameter **openssh**: Uses the format of OpenSSH.

ssh1: Uses the format of SSH1.

ssh2: Uses the format of SSH2.

filename: Name of the file for storing public key.

Description Use the **public-key local export rsa** command to display the local RSA public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the local RSA public key on the screen; otherwise, the command exports the local RSA public key to the specified file and saves the file.

SSH1, SSH2 and OpenSSH are three different public key file formats for different requirements.

Related command: **public-key local create**, **public-key local destroy**.

Example # Export the local RSA public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh key.pub
```

Display the local RSA public key in SSH2 format.

```
<Sysname> system-view
[Sysname] public-key local export rsa ssh2
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "rsa-key-20061105"
AAAAB3NzaC1yc2EAAAADAQABAAAAgKRkxFoZ+T72Srs9c60+j2yrkd0AHBsXBh0Uq+iN
vE12PaYR1On4
x+aNlwe9fjW1PYgzH+DRkTpiMrn3j2pIs7gaJXvefTW94rbVWJ94uiSDk1NLX1JcoTtW
nQcVhft3mUZ+
J0jBEhAcw4bROe7/qr6l7VTCo9FBZ0XgKuHroovX
---- END SSH2 PUBLIC KEY ----
```

Display the RSA local public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export rsa openssh
ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAAAgLxMOSqXc0pjO6Dx2wH4TrUSKOyGreHb
pZfg2QZv3E8Ed2zqNhDSV4NB9dBJFDZW8Sh1AsBtOdOfKPD1y6Yw2ozRwW7OinplKC8k
B+h1fnk33M2122IM0fRxQBtxFxOXAjSERKLYkASXqHuNXxPWHE3vo9FKfcB2JHkfwdIm
9i3z rsa-key
```

public-key local export dsa

Syntax **public-key local export dsa** { **openssh** | **ssh2** } [*filename*]

View System view

Parameter **openssh**: Uses the format of OpenSSH.

ssh2: Uses the format of SSH2.

filename: Name of the file for storing public key. The value range varies by devices.

Description Use the **public-key local export dsa** command to display the DSA local public key on the screen or export it to a specified file.

If you do not specify the *filename* argument, the command displays the DSA local public key on the screen; otherwise, the command exports the DSA local public key to the specified file and saves the file.

SSH2 and OpenSSH are two different public key file formats for different requirements.

Related command: **public-key local create**, **public-key local destroy**.

Example # Export the DSA local public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh key.pub
```

Display the DSA local public key in SSH2 format.

```
<Sysname> system-view
[Sysname] public-key local export dsa ssh2
```

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "dsa-key-20061025"
AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9yzhSg06Ui
L+CM7OZb5sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG/WD+AZQd
3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAAFQDHcyGM
c37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN/OrpbsTV
75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGscXthI5HH
bB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmwnu8AAACB
AMoAntnKNEUhJUyMhEr0bji4MelDmsZyDaadRG7UONHs6gN/0aLYE/ptjKQvesXdKbv+
FDnLq5C91bsBxXS3C1CEtF8ifxm60kUQz7T3R0+r5xEjRaFrwdxxTk9Vwpvzm1SPJa9V
8W4A0dt3xksktTU51303szQVrD1cMMYZ5YAU
---- END SSH2 PUBLIC KEY ----
```

Display the DSA local public key in OpenSSH format.

```
<Sysname> system-view
[Sysname] public-key local export dsa openssh
ssh-dss AAAAB3NzaC1kc3MAAACBANdXJixFhMRMIR8YvZbl8GHE8KQj9/5ra4WzTO9y
zhSg06UiL+CM7OZb5sJlhUiJ3B7b0T7IsnTan3W6Jsy5h3I2Anh+kiuoRCHyLDyJy5sG
/WD+AZQd3Xf+axKJPadu68HRKNl/BnjXcitTQchQbzWCFLFqL6xLNolQOHgRx9ozAAAA
FQDHcyGMc37I7pk7Ty3tMPSO2s6RXwAAAIEAgiaQCeFOxHS68pMuadOx8YUXrZWUGEzN
/OrpbsTV75MTPoS0cJPFKyDNNdAkkrOVnsZJliW8T6UILiLFs3ThbdABMs5xsCAhcJGs
cXthI5HHbB+y6IMXwb2BcdQey4PiEMA8ybMugQVhwhYhxz1tqsAo9LFYXaf0JRlxjMmw
nu8AAACBAMoAntnKNEUhJUyMhEr0bji4MelDmsZyDaadRG7UONHs6gN/0aLYE/ptjKQv
esXdKbv+FDnLq5C91bsBxXS3C1CEtF8ifxm60kUQz7T3R0+r5xEjRaFrwdxxTk9Vwpvz
m1SPJa9V8W4A0dt3xksktTU51303szQVrD1cMMYZ5YAU dsa-key
```

public-key peer

Syntax **public-key peer** *keyname*

undo public-key peer *keyname*

View System view

Parameter *keyname*: Public key name, a string of 1 to 64 characters.

Description Use the **public-key peer** command to enter public key view.

Use the **undo public-key peer** command to delete the configuration of peer public key.

After entering public key view, you can configure the peer public key with the **public-key-code begin** and **public-key-code end** commands. This requires that you obtain the hexadecimal public key from the peer beforehand.

Related command: **public-key-code begin**, **public-key-code end**.

Example # Enter public key view, specifying a public key **key1**.

```
<Sysname> system-view
[Sysname] public-key peer key1
[Sysname-pkey-public-key]
```

public-key peer import sshkey

Syntax **public-key peer** *keyname* **import sshkey** *filename*

undo public-key peer *keyname*

View System view

Parameter *keyname*: Public key name, a string of 1 to 64 characters.

filename: Public key file name. The value range varies by device models.

Description Use the **public-key peer import sshkey** command to import a peer public key from the public key file.

Use the **undo public-key peer import sshkey** command to remove the setting.

After execution of this command, the system automatically transforms the public key file in SSH1, SSH2 or OpenSSH format to PKCS format, and imports the peer public key. This requires that you get a copy of the public key file from the peer through FTP/TFTP.

Example # Import a peer public key named **key2** from public key file **key.pub**.

```
<Sysname> system-view
[Sysname] public-key peer key2 import sshkey key.pub
```

sftp

Syntax **sftp** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameter *server*: IPv4 address or name of the server, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.

- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **sftp** command to establish a connection to a remote IPv4 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Example # Connect to SFTP server 10.1.1.2.

```
<Sysname> sftp 10.1.1.2
Input Username:
```

sftp client ipv6 source

Syntax **sftp client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo sftp client ipv6 source

View System view

Parameter **ipv6** *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **sftp client ipv6 source** command to specify the source IPv6 address or source interface for an SFTP client.

Use the **undo sftp client ipv6 source** command to remove the configuration.

By default, the client uses the interface address specified by the route of the device to access the SFTP server.

Example # Specify the source IPv6 address of the SFTP client as 2:2::2:2.

```
<Sysname> system-view
[Sysname] sftp client ipv6 source ipv6 2:2::2:2
```

sftp client source

Syntax **sftp client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo sftp client source

View System view

Parameter **ip** *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **sftp client source** command to specify the source IPv4 address or interface of an SFTP client.

Use the **undo sftp source-interface** command to remove the configuration.

By default, a client uses the IP address or interface specified by the route to access the SFTP server.

Related command: **display sftp client source**.

Example # Specify the source IP address of the SFTP client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] sftp client source ip 192.168.0.1
```

sftp ipv6

Syntax **sftp ipv6** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameter *server*: IPv6 address or name of the server, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **sftp ipv6** command to establish a connection to a remote IPv6 SFTP server and enter SFTP client view.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Example # Connect to server 2:5::8:9.

```
<Sysname> sftp ipv6 2:5::8:9
Input Username:
```

sftp server enable

Syntax **sftp server enable**

undo sftp server enable

View System view

Parameter None

Description Use the **sftp server enable** command to enable SFTP server.

Use the **undo sftp server enable** command to disable SFTP server.

By default, SFTP server is disabled.

Related command: **display ssh server**.

Example # Enable SFTP server.

```
<Sysname> system-view
[Sysname] sftp server enable
```

sftp server idle-timeout

Syntax **sftp server idle-timeout** *time-out-value*

undo sftp server idle-timeout

View System view

Parameter *time-out-value*: Timeout period in minutes. It ranges from 1 to 35,791.

Description Use the **sftp server idle-timeout** command to set the idle timeout period for SFTP user connections.

Use the **undo sftp server idle-timeout** command to restore the default.

By default, the idle timeout period is 10 minutes.

Related command: **display ssh server**.

Example # Set the idle timeout period for SFTP user connections to 500 minutes.

```
<Sysname> system-view
[Sysname] sftp server idle-timeout 500
```

ssh client authentication server

Syntax **ssh client authentication server** *server* **assign publickey** *keyname*

undo ssh client authentication server *server* **assign publickey**

View System view

Parameter *server*: IP address or name of the server, a string of 1 to 80 characters.

assign publickey *keyname*: Specifies the name of the host public key of the server, which is a string of 1 to 64 characters.

Description Use the **ssh client authentication server** command to configure the host public key of the server so that the client can determine whether the server is trustworthy.

Use the **undo ssh authentication server** command to remove the configuration.

By default, the host public key of the server is not configured, and when logging into the server, the client uses the IP address or host name used for login as the public key name.

Example # Configure the public key of the server with the IP address of 192.168.0.1 to be **key1**.

```
<Sysname> system-view
[Sysname] ssh client authentication server 192.168.0.1 assign rsa-key key1
```

ssh client first-time enable

Syntax **ssh client first-time enable**

undo ssh client first-time

View System view

Parameter None

Description Use the **ssh client first-time enable** command to enable the first authentication function.

Use the **undo ssh client first-time** command to disable the function.

By default, the function is enabled.

When an SSH client tries to access a server whose public host key it does not know for the first time, the first authentication function enables it to access the server and obtain and save the public host key of the server. When the client accesses the

server later, it can use the locally saved public host key of the server to authenticate the server.

With the first authentication function disabled, an SSH client cannot access any server whose public host key it does not know. In this case, you must configure the public host key of the server to be accessed and specify the public key name on the client at first.

Example # Enable the first authentication function.

```
<Sysname> system-view
[Sysname] ssh client first-time enable
```

ssh client ipv6 source

Syntax **ssh client ipv6 source** { **ipv6** *ipv6-address* | **interface** *interface-type interface-number* }

undo ssh client ipv6 source

View System view

Parameter **ipv6** *ipv6-address*: Specifies a source IPv6 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **ssh client ipv6 source** command to specify the source IPv6 address or source interface for the SSH client.

Use the **undo ssh client ipv6 source** command to remove the configuration.

By default, the client uses the source address specified by the route of the device to access the SSH server.

Example # Specify the source IPv6 address as 2:2::2:2 for the SSH client.

```
<Sysname> system-view
[Sysname] ssh client ipv6 source ipv6 2:2::2:2
```

ssh client source

Syntax **ssh client source** { **ip** *ip-address* | **interface** *interface-type interface-number* }

undo ssh client source

View System view

Parameter **ip** *ip-address*: Specifies a source IPv4 address.

interface *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **ssh client source** command to specify the source IPv4 address or source interface of the SSH client.

Use the **undo ssh client source** command to remove the configuration.

By default, an SSH client uses the IP address or interface specified by the route to access the SSH server.

Related command: **display ssh client source**.

Example # Specify the source IPv4 address of the SSH client as 192.168.0.1.

```
<Sysname> system-view
[Sysname] ssh client source ip 192.168.0.1
```

ssh server authentication-retries

Syntax **ssh server authentication-retries** *times*

undo ssh server authentication-retries

View System view

Parameter *times:* Maximum number of authentication attempts, in the range 1 to 5.

Description Use the **ssh server authentication-retries** command to set the maximum number of SSH connection authentication attempts, which takes effect at next login.

Use the **undo ssh server authentication-retries** command to restore the default.

By default, the maximum number of SSH connection authentication attempts is 3.

Note that the threshold specified by using the **ssh server authentication-retries** command takes into account both publickey authentication attempts and password authentication attempts.

Related command: **display ssh server**.

Example # Set the maximum number of SSH connection authentication attempts to 4.

```
<Sysname> system-view
[Sysname] ssh server authentication-retries 4
```

ssh server authentication-timeout

Syntax **ssh server authentication-timeout** *time-out-value*

undo ssh server authentication-timeout

View System view

Parameter *time-out-value*: Authentication timeout period in seconds, in the range 1 to120.

Description Use the **ssh server authentication-timeout** command to set the SSH user authentication timeout period on the SSH server.

Use the **undo ssh server authentication-timeout** command to restore the default.

By default, the authentication timeout period is 60 seconds.

Related command: **display ssh server**.

Example # Set the SSH user authentication timeout period to 10 seconds.

```
<Sysname> system-view
[Sysname] ssh server authentication-timeout 10
```

ssh server compatible-ssh1x enable

Syntax **ssh server compatible-ssh1x enable**

undo ssh server compatible-ssh1x

View System view

Parameter None

Description Use the **ssh server compatible-ssh1x** command to enable the SSH server to work with SSH1.x clients.

Use the **undo ssh server compatible-ssh1x** command to disable the SSH server from working with SSH1.x clients.

By default, the SSH server can work with SSH1.x clients.

This configuration takes effect at next login.

Related command: **display ssh server**.

Example # Enable the SSH server to work with SSH1.x clients.

```
<Sysname> system-view
[Sysname] ssh server compatible-ssh1x enable
```

ssh server enable

Syntax **ssh server enable**

undo ssh server enable

View System view

Parameter None

Description Use the **ssh server enable** command to enable SSH server.

Use the **undo ssh server enable** command to disable SSH server.

By default, SSH server is disabled.

Example # Enable SSH server.

```
<Sysname> system-view
[Sysname] ssh server enable
```

ssh server rekey-interval

Syntax **ssh server rekey-interval** *hours*

undo ssh server rekey-interval

View System view

Parameter *hours:* Server key pair update interval in hours, in the range 1 to 24.

Description Use the **ssh server rekey-interval** command to set the interval for updating the RSA server key.

Use the **undo ssh server rekey-interval** command to remove the configuration.

By default, the update interval of the RSA server key is 0, that is, the RSA server key is not updated.

Related command: **display ssh server**.

CAUTION: This command is only available to SSH users using SSH1 client software.

Example # Set the RSA server key update interval to three hours.

```
<Sysname> system-view
[Sysname] ssh server rekey-interval 3
```

ssh user

Syntax

ssh user *username* **service-type stelnet authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* }

ssh user *username* **service-type** { **all** | **sftp** } **authentication-type** { **password** | { **any** | **password-publickey** | **publickey** } **assign publickey** *keyname* **work-directory** *directory-name* }

undo ssh user *username*

View

System view

Parameter

username: SSH username, a string of 1 to 80 characters.

service-type: Specifies the service type of an SSH user, which can be one of the following:

- **all**: Specifies both secure Telnet and secure FTP.
- **sftp**: Specifies the service type as secure FTP.
- **stelnet**: Specifies the service type of secure Telnet.
- **authentication-type**: Specifies the authentication method of an SSH user, which can be one the following:
- **password**: Performs password authentication.
- **any**: Performs either password authentication or publickey authentication. The client tries publickey authentication first.
- **password-publickey**: Performs both password authentication and publickey authentication. A client running SSH1 client only needs to pass either type of authentication while a client running SSH2 client must pass both types of authentication to log in.
- **publickey**: Performs publickey authentication.

assign publickey *keyname*: Assigns an existing public key for an SSH user. The key name is a string of 1 to 64 characters.

work-directory *directory-name*: Specifies a work folder for an SFTP user. The folder name is a string of 1 to 135 characters.

Description

Use the **ssh user** command to create an SSH user and specify the service type and authentication method.

Use the **undo ssh user assign rsa-key** command to delete the SSH user.

Use the **undo ssh user** *username* command to delete a user.

Note that:

- For a publickey authentication user, you must configure the username and the public key on the device. For a password authentication user, you can configure the account information on either the device or the remote authentication server such as a RADIUS server.
- If you use the **ssh user** command to configure a public key for a user who has already had a public key, the new one overwrites the old one.
- The new public key takes effect when the user logs in next time.
- If an SFTP user has been assigned a public key, it is necessary to set a working folder for the user.
- The working folder of an SFTP user is subject to the user authentication method. For a user using only password authentication, the working folder is the AAA authorized one. For a user using only publickey authentication or using both the publickey and password authentication methods, the working folder is the one set by using the **ssh user** command.

Related command: **display ssh user-information**.

Example # Create an SSH user named **user1**, and specify the service type as **sftp**, the authentication method as **publickey**, the work folder of the SFTP server as **flash**, and assign a public key named **key1** to the user.

```
<Sysname> system-view
[Sysname] ssh user user1 service-type sftp athentication-type public
key assign publickey key1 work-directory flash:
```

ssh2

Syntax **ssh2** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameter *server*: IPv4 address or name of the server, a string of 1 to 20 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, defaulted to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-group1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-group14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2** command to establish a connection to an SSH server, and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Example # Login to remote SSH2 server 10.214.50.51, setting the algorithms as follows:

- Preferred key exchange algorithm: **dh-group1**
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5
- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 10.214.50.51 prefer-kex dh-group 1 prefer-stoc-cipher
 aes128 prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

ssh2 ipv6

Syntax **ssh2 ipv6** *server* [*port-number*] [**identity-key** { **dsa** | **rsa** } | **prefer-ctos-cipher** { **3des** | **aes128** | **des** } | **prefer-ctos-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** } | **prefer-kex** { **dh-group-exchange** | **dh-group1** | **dh-group14** } | **prefer-stoc-cipher** { **3des** | **aes128** | **des** } | **prefer-stoc-hmac** { **md5** | **md5-96** | **sha1** | **sha1-96** }] *

View User view

Parameter *server*: IPv6 address or name of the server, a string of 1 to 46 characters.

port-number: Port number of the server, in the range 0 to 65535. The default is 22.

identity-key: Specifies the algorithm for publickey authentication, either **dsa** or **rsa**. The default is **dsa**.

prefer-ctos-cipher: Preferred encryption algorithm from client to server, defaulted to **aes128**.

- **3des**: Encryption algorithm 3des-cbc.
- **aes128**: Encryption algorithm aes128-cbc.
- **des**: Encryption algorithm des-cbc.

prefer-ctos-hmac: Preferred HMAC algorithm from client to server, defaulted to **sha1**.

- **md5**: HMAC algorithm hmac-md5.
- **md5-96**: HMAC algorithm hmac-md5-96.
- **sha1**: HMAC algorithm hmac-sha1.
- **sha1-96**: HMAC algorithm hmac-sha1-96.

prefer-kex: Preferred key exchange algorithm, default to **dh-group-exchange**.

- **dh-group-exchange**: Key exchange algorithm diffie-hellman-group-exchange-sha1.
- **dh-roup1**: Key exchange algorithm diffie-hellman-group1-sha1.
- **dh-roup14**: Key exchange algorithm diffie-hellman-group14-sha1.

prefer-stoc-cipher: Preferred encryption algorithm from server to client, defaulted to **aes128**.

prefer-stoc-hmac: Preferred HMAC algorithm from server to client, defaulted to **sha1**.

Description Use the **ssh2 ipv6** command to establish a connection to an IPv6 SSH server and specify the preferred key exchange algorithm, encryption algorithms, and HMAC algorithms of the client and the server.

Note that when the client's authentication method is publickey, the client needs to get the local private key for validation. As the publickey authentication includes RSA and DSA algorithms, you must specify an algorithm (by using the **identity-key** keyword) in order to get the correct data for the local private key.

Example # Login to remote SSH2 server 2000::1, setting the algorithms as follows:

- Preferred key exchange algorithm: **dh-group1**
- Preferred encryption algorithm from server to client: AES128
- Preferred HMAC algorithm from client to server: MD5

- Preferred HMAC algorithm from server to client: SHA1-96.

```
<Sysname> ssh2 ipv6 2000::1 prefer-kex dh-group 1 prefer-stoc-cipher
 aes128 prefer-ctos-hmac md5 prefer-stoc-hmac sha1-96
```

143
SFTP CONFIGURATION COMMANDS

bye

Syntax **bye**

View SFTP client view

Parameter None

Description Use the **bye** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **exit** and **quit** commands.

Example # Terminate the connection with the remote SFTP server.

```
sftp-client> bye
Bye
[Sysname]
```

cd

Syntax **cd** [*remote-path*]

View SFTP client view

Parameter *remote-path*: Name of a path on the server.

Description Use the **cd** command to change the working path on a remote SFTP server. With the argument not specified, the command displays the current working path.

- *You can use the **cd ..** command to return to the upper-level directory.*
- *You can use the **cd /** command to return to the root directory of the system.*

Example # Change the working path to **new1**.

```
sftp-client> cd new1
Current Directory is:
/new1
```

cdup

Syntax **cdup**

View SFTP client view

Parameter None

Description Use the **cdup** command to return to the upper-level directory.

Example # From the current working directory **/new1**, return to the upper-level directory.

```
sftp-client> cdup
Current Directory is:
/
```

delete

Syntax **delete** *remote-file*&<1-10>

View SFTP client view

Parameter *remote-file*&<1-10>: Name of a file on the server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **delete** command to delete a specified file from a server.

This command functions as the **remove** command.

Example # Delete file **temp.c** from the server.

```
sftp-client> delete temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

dir

Syntax **dir** [**-a** | **-l**] [*remote-path*]

View SFTP client view

Parameter **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory

remote-path: Name of the directory to be queried.

Description Use the **dir** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **ls** command.

Example # Display in a list form detailed file and folder information under the current working directory.

```
sftp-client> dir
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

exit

Syntax **exit**

View SFTP client view

Parameter None

Description Use the **exit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **quit** commands.

Example # Terminate the connection with the remote SFTP server.

```
sftp-client> exit
Bye
[Sysname]
```

get

Syntax **get** *remote-file* [*local-file*]

View SFTP client view

Parameter *remote-file*: Name of a file on the remote SFTP server.

local-file: Name for the local file.

Description Use the **get** command to download a file from a remote SFTP server and save it locally.

If you do not specify the *local-file* argument, the file will be saved locally with the same name as that on the remote SFTP server.

Example # Download file **temp1.c** and save it as **temp.c** locally.

```
sftp-client> get temp1.c temp.c
Remote  file:/temp1.c --->  Local file: temp.c
Downloading file successfully ended
```

help

Syntax **help** [**all** | *command-name*]

View SFTP client view

Parameter **all**: Displays a list of all commands.

command-name: Name of a command.

Description Use the **help** command to display a list of all commands or the help information of an SFTP client command.

With neither the argument nor the keyword specified, the command displays a list of all commands.

Example # Display the help information of the **get** command.

```
sftp-client> help get
get remote-path [local-path]  Download file
Default local-path is the same with remote-path
```

ls

Syntax **ls** [**-a** | **-l**] [*remote-path*]

View SFTP client view

Parameter **-a**: Displays the filenames or the folder names of the specified directory.

-l: Displays in list form detailed information of the files and folder of the specified directory

remote-path: Name of the directory to be queried.

Description Use the **ls** command to display file and folder information under a specified directory.

With the **-a** and **-l** keyword not specified, the command displays detailed information of files and folder under the specified directory in a list form.

With the *remote-path* not specified, the command displays the file and folder information of the current working directory.

This command functions as the **dir** command.

Example # Display in a list form the detailed file and folder information under the current working directory.

```
sftp-client> ls
-rwxrwxrwx   1 noone    nogroup      1759 Aug 23 06:52 config.cfg
-rwxrwxrwx   1 noone    nogroup       225 Aug 24 08:01 pubkey2
-rwxrwxrwx   1 noone    nogroup       283 Aug 24 07:39 pubkey1
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:28 pub1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:24 new1
drwxrwxrwx   1 noone    nogroup         0 Sep 28 08:18 new2
-rwxrwxrwx   1 noone    nogroup       225 Sep 28 08:30 pub2
```

mkdir

Syntax **mkdir** *remote-path*

View SFTP client view

Parameter *remote-path*: Name for the directory on a remote SFTP server.

Description Use the **mkdir** command to create a directory on a remote SFTP server.

Example # Create a directory named **test** on the remote SFTP server.

```
sftp-client> mkdir test
New directory created
```

put

Syntax **put** *local-file* [*remote-file*]

View SFTP client view

Parameter *local-file*: Name of a local file.

remote-file: Name for the file on a remote SFTP server.

Description Use the **put** command to upload a local file to a remote SFTP server.

If you do not specify the *remote-file* argument, the file will be saved remotely with the same name as the local one.

Example # Upload local file **temp.c** to the remote SFTP server and save it as **temp1.c**.

```
sftp-client> put temp.c temp1.c
Local file:temp.c --->  Remote file: /temp1.c
Uploading file successfully ended
```

pwd

Syntax **pwd**

View SFTP client view

Parameter None

Description Use the **pwd** command to display the current working directory of a remote SFTP server.

Example # Display the current working directory of the remote SFTP server.

```
sftp-client> pwd
/
```

quit

Syntax **quit**

View SFTP client view

Parameter None

Description Use the **quit** command to terminate the connection with a remote SFTP server and return to system view.

This command functions as the **bye** and **exit** commands.

Example # Terminate the connection with the remote SFTP server.

```
sftp-client> quit
Bye
[Sysname]
```

remove

Syntax **remove** *remote-file*&<1-10>

View SFTP client view

Parameter *remote-file*&<1-10>: Name of a file on an SFTP server. &<1-10> means that you can provide up to 10 filenames, which are separated by space.

Description Use the **remove** command to delete a specified file from a remote server.

This command functions as the **delete** command.

Example # Delete file **temp.c** from the server.

```
sftp-client> remove temp.c
The following files will be deleted:
/temp.c
Are you sure to delete it? [Y/N]:y
This operation may take a long time.Please wait...

File successfully Removed
```

rename

Syntax **rename** *oldname newname*

View SFTP client view

Parameter *oldname*: Original file name or directory name.

newname: New file name or directory name.

Description Use the **rename** command to change the name of a specified file or directory on an SFTP server.

Example # Change the name of a file on the SFTP server from **temp1.c** to **temp2.c**.

```
sftp-client> rename temp1.c temp2.c
File successfully renamed
```

rmdir

Syntax **rmdir** *remote-path*&<1-10>

View SFTP client view

Parameter *remote-path*&<1-10>: Name of the directory on the remote SFTP server. &<1-10> means that you can provide up to 10 filenames that are separated by space.

Description Use the **rmdir** command to delete a specified directory from an SFTP server.

Example # On the SFTP server, delete directory **temp1** in the current directory.

```
sftp-client> rmdir temp1
Directory successfully removed
```

144 SSL CONFIGURATION COMMANDS

ciphersuite

Syntax **ciphersuite [rsa_3des_ede_cbc_sha | rsa_aes_128_cbc_sha | rsa_aes_256_cbc_sha | rsa_des_cbc_sha | rsa_rc4_128_md5 | rsa_rc4_128_sha] ***

View SSL server policy view

Parameter **rsa_3des_ede_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC and the MAC algorithm of SHA.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm 256-bit AES_CBC, and the MAC algorithm of SHA.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description Use the **ciphersuite** command to specify the cipher suite(s) for an SSL server policy to support.

By default, an SSL server policy supports all cipher suites.

With no keyword specified, the command configures an SSL server policy to support all cipher suites.

Example # Specify the cipher suites for SSL server policy policy1 to support as **rsa_rc4_128_md5** and **rsa_rc4_128_sha**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] ciphersuite rsa_rc4_128_md5 rsa_rc4_128_sha
```

client-verify enable

Syntax **client-verify enable**

undo client-verify enable

View SSL server policy view

Parameter None

Description Use the **client-verify enable** command to enable certificate-based SSL client authentication, that is, to enable the SSL server to perform certificate-based authentication of the client during the SSL handshake process.

Use the **undo client-verify enable** command to restore the default.

By default, certificate-based SSL client authentication is disabled.

Example # Enable certificate-based client authentication.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] client-verify enable
```

close-mode wait

Syntax **close-mode wait**

undo close-mode wait

View SSL server policy view

Parameter None

Description Use the **close-mode wait** command to set the SSL connection close mode to **wait**. In this mode, after sending a close-notify message to a client, the server does not close the connection until it receives a close-notify message from the client.

Use the **undo close-mode wait** command to restore the default.

By default, an SSL server sends a close-notify alert message to the client and close the connection without waiting for the close-notify alert message from the client.

Example # Set the SSL connection close mode to **wait**.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] close-mode wait
```

display ssl client-policy

Syntax **display ssl client-policy** { *policy-name* | **all** }

View Any view

Parameter *policy-name*: SSL client policy name, a string of 1 to 16 characters.

all: Displays information about all SSL client policies.

Description Use the **display ssl client-policy** command to view information about a specified or all SSL client policies.

Example # Display information about SSL client policy policy1.

```
<Sysname> display ssl client-policy policy1
 SSL Client Policy: policy1
     SSL Version: SSL 3.0
     PKI Domain: 1
     Prefer Ciphersuite:
         RSA_RC4_128_SHA
```

Table 580 Description on the fields of the display ssl client-policy command

Field	Description
SSL Client Policy	SSL client policy name
SSL Version	Version of the protocol adopted by the SSL client policy
PKI Domain	PKI domain of the SSL client policy
Prefer Ciphersuite	Preferred cipher suite of the SSL client policy

display ssl server-policy

Syntax **display ssl server-policy** { *policy-name* | **all** }

View Any view

Parameter *policy-name*: SSL server policy name, a string of 1 to 16 characters.

all: Displays information about all SSL server policies.

Description Use the **display ssl server-policy** command to view information about a specified or all SSL server policies.

Example # Display information about SSL server policy policy1.

```
<Sysname> display ssl server-policy policy1
 SSL Server Policy: policy1
     PKI Domain: domain1
     Ciphersuite:
         RSA_RC4_128_MD5
```

```
        RSA_RC4_128_SHA
        RSA_DES_CBC_SHA
        RSA_3DES_EDE_CBC_SHA
        RSA_AES_128_CBC_SHA
        RSA_AES_256_CBC_SHA
    Handshake Timeout: 3600
    Close-mode: wait disabled
    Session Timeout: 3600
    Session Cachesize: 500
    Client-verify: disabled
```

Table 581 Description on the fields of the display ssl server-policy command

Field	Description
SSL Server Policy	SSL server policy name
PKI Domain	PKI domain to which the SSL server policy belongs
Ciphersuite	Cipher suites supported by the SSL server policy
Handshake Timeout	Handshake timeout time of the SSL server policy
Close-mode	Close mode of the SSL server policy
Session Timeout	Session timeout time of the SSL server policy
Session Cachesize	Maximum number of buffered sessions of the SSL server policy
Client-verify	Whether client authentication is enabled

handshake timeout

Syntax **handshake timeout** *time*

undo handshake timeout

View SSL server policy view

Parameter *time*: Handshake timeout time, in the range 180 to 7,200 seconds.

Description Use the **handshake timeout** command to set the handshake timeout time for an SSL server policy.

Use the **undo handshake timeout** command to restore the default.

By default, the handshake timeout time is 3,600 seconds.

Example # Set the handshake timeout time of SSL server policy policy1 to 3,000 seconds.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] handshake timeout 3000
```

pki-domain

Syntax **pki-domain** *domain-name*

undo pki-domain

View SSL server policy view/SSL client policy view

Parameter *domain*-name: Name of a PKI domain, a string of 1 to 15 characters.

Description Use the **pki-domain** command to specify a PKI domain for an SSL server policy or SSL client policy.

Use the **undo pki-domain** command to restore the default.

By default, no PKI domain is configured for an SSL server policy or SSL client policy by default.

Example # Configure SSL server policy policy1 to use the PKI domain named server-domain.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] pki-domain server-domain
```

Configure SSL client policy policy1 to use the PKI domain named client-domain.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] pki-domain client-domain
```

prefer-cipher

Syntax **prefer-cipher** { **rsa_3des_ede_cbc_sha** | **rsa_aes_128_cbc_sha** | **rsa_aes_256_cbc_sha** | **rsa_des_cbc_sha** | **rsa_rc4_128_md5** | **rsa_rc4_128_sha** }

undo prefer-cipher

View SSL client policy view

Parameter **rsa_3des_ede_cbc_sha**: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 3DES_EDE_CBC, and the MAC algorithm of SHA. Support for this keyword varies by device.

rsa_aes_128_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit AES_CBC, and the MAC algorithm of SHA.

rsa_aes_256_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 256-bit AES_CBC, and the MAC algorithm of SHA. Support for this keyword varies by device.

rsa_des_cbc_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of DES_CBC, and the MAC algorithm of SHA.

rsa_rc4_128_md5: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of MD5.

rsa_rc4_128_sha: Specifies the key exchange algorithm of RSA, the data encryption algorithm of 128-bit RC4, and the MAC algorithm of SHA.

Description Use the **prefer-cipher** command to specify the preferred cipher suite for an SSL client policy.

Use the **undo prefer-cipher** command to restore the default.

By default, the preferred cipher suite for an SSL client policy is **rsa_rc4_128_md5**.

Example # Set the preferred cipher suite for SSL client policy policy1 to **rsa_aes_128_cbc_sha**.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] prefer-cipher rsa_aes_128_cbc_sha
```

session

Syntax **session** { **cachesize** *size* | **timeout** *time* } *

undo session { **cachesize** | **timeout** } *

View SSL server policy view

Parameter **cachesize** *size*: Sets the maximum number of cached sessions, in the range 100 to 1,000.

timeout *time*: Sets the caching timeout time, in the range 1,800 to 72,000 seconds.

Description Use the **session** command to set the maximum number of cached sessions and the caching timeout time.

Use the **undo session** command to restore the default.

By default, the maximum number of cached sessions is 500 and the caching timeout time is 3,600 seconds.

If the number of sessions in the cache reaches the maximum, SSL rejects to cache new sessions. If a session exists in the cache for a period equal to the caching timeout time, SSL removes it from the cache.

Example # Set the caching timeout time to 4,000 seconds, and the maximum number of cached sessions to 600.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1] session timeout 4000 cachesize 600
```

ssl client-policy

Syntax **ssl client-policy** *policy-name*

undo ssl client-policy { *policy-name* | **all** }

View System view

Parameter *policy-name:* SSL client policy name, a case-insensitive string of 1 to 16 characters, which cannot be "a", "al" and "all".

all: Specifies all SSL client policies.

Description Use the **ssl client-policy** command to create an SSL policy and enter its view.

Use the **undo ssl client-policy** command to remove a specified or all SSL client policies.

Example # Create an SSL client policy named policy1 and enter its view.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1]
```

ssl server-policy

Syntax **ssl server-policy** *policy-name*

undo ssl server-policy { *policy-name* | **all** }

View System view

Parameter *policy-name:* SSL server policy name, a case-insensitive string of 1 to 16 characters, which cannot be "a", "al" and "all".

all: Specifies all SSL server policies.

Description Use the **ssl server-policy** command to create an SSL server policy and enter its view.

Use the **undo ssl server-policy** command to remove a specified or all SSL server policies.

Note that you cannot delete an SSL server policy that has been associated with one or more application layer protocols.

Example # Create an SSL server policy named policy1 and enter its view.

```
<Sysname> system-view
[Sysname] ssl server-policy policy1
[Sysname-ssl-server-policy-policy1]
```

version

Syntax **version** { **ssl3.0** | **tls1.0** }

undo version

View SSL client policy view

Parameter **ssl3.0**: Specifies SSL 3.0.

tls1.0: Specifies TLS 1.0.

Description Use the **version** command to specify the SSL protocol version for an SSL client policy.

Use the **undo version** command to restore the default.

By default, the SSL protocol version for an SSL client policy is TLS 1.0.

Example # Specify the SSL protocol version for SSL client policy policy1 as SSL 3.0.

```
<Sysname> system-view
[Sysname] ssl client-policy policy1
[Sysname-ssl-client-policy-policy1] version ssl3.0
```

145 BACKUP CENTER CONFIGURATION COMMANDS

display standby flow

Syntax **display standby flow**

View Any view

Parameter None

Description Use the **display standby flow** command to display statistics about traffic on the main interfaces participating in load sharing.

Example # Display statistics about the traffic on the main interfaces participating in load sharing.

```
<Sysname> display standby flow
Interfacename : Serial2/0
Flow-interval(s) : 100
LastInOctets : 868168
LastOutOctets : 1818667
InFlow(Octets) : 50070
OutFlow(Octets) : 100088
BandWidth(b/s) : 9000
UsedBandWidth(b/s) : 8000
```

Table 582 Description on the fields of the display standby flow command

Field	Description
Interfacename	Name of the main interface
Flow-interval(s)	Intervals for checking traffic on the main interface
LastInOctets	Sum of the octets received on the main interface until the last check
LastOutOctets	Sum of the octets sent on the main interface until the last check
InFlow(Octets)	Sum of the octets received on the main interface during the last interval
OutFlow(Octets)	Sum of the octets sent on the main interface during the last interval
BandWidth(b/s)	Bandwidth of the main interface
UsedBandWidth(b/s)	Actual bandwidth for the main interface participating in load sharing during the last interval

display standby state

Syntax **display standby state**

View Any view

Parameter None

Description Use the **display standby state** command to display the state information of the main and backup interfaces.

Example # Display the state information of the main and backup interfaces.

```
<Sysname> display standby state
Interface     Interfacestate Backupstate Backupflag Pri Loadstate
Serial2/0      UP             MUP         MUD             TO-HYPNOTIZE
Serial2/1      DOWN           DOWM        BU         30
Serial2/2      STANDBY        STANDBY     BU         10

Backup-flag meaning:
M---MAIN  B---BACKUP     V---MOVED    U---USED
D---LOAD  P---PULLED
```

The following tables describe the meanings of each state.

Table 583 States of main and backup interfaces

State	Main interface	Backup interface
Up	Indicates that the physical link is functioning normally for data transmission.	
Down	Indicates that the physical link is not available for data transmission, for example, because no cable connection is present.	
Standby	--	The state of the backup interface when the main interface is functioning. Data transmission is disabled on the backup interface.

Table 584 Backup states of the main interface

State	Description
MUP	The main interface is working normally for data transmission.
MUPDELAY	The main interface is experiencing a delay before it transits from the non-working state to the working state to take over. At this time, the backup interface is still active.
MDOWN	The main interface cannot work normally. A backup interface must be brought up to take over.
MDOWNDELAY	The main interface is experiencing a delay before it transits from the working state to the non-working state. At this time, the backup interface does not really take over the job of the main interface.

Table 585 Backup states of the backup interface

State	Description
UP	State of the backup interface when it is started

Table 585 Backup states of the backup interface

State	Description
UPDELAY	The backup interface is experiencing a delay before it transits from the non-working state to the working state to take over.
DOWN	The backup interface cannot work normally.
DOWNDELAY	The backup interface is experiencing a delay before it transits from the working state to the non-working state. At this time, the backup interface is probably still working.
STANDBY	State of the backup interface when the main interface is working. At this time, the backup interface cannot send or receive data.

Table 586 Backup flags

Flag	Description
M---MAIN	Indicates that the interface is a main one.
B---BACKUP	Indicates that the interface is a backup one.
V---MOVED	Indicates that the interface or the main interface of the interface, or all backup interfaces of the interface are all removed.
U---USED	Indicates that the interface is being used as a main interface or backup interface.
D---LOAD	Indicates that the main interface participates in load sharing.
P---PULLED	Indicates that the interface board where the interface is located is removed.

Table 587 Load sharing states

State	Description
WAKE	The backup interface is working in the load sharing state to transmit data together with the main interface.
TO-HYPNOTIZE	The backup interface is transiting from the working state to the non-working state after the traffic size decreases below the lower backup load sharing threshold. In this state, the backup interface is still working.
TO-WAKE	The backup interface is transiting from the non-working state to the working state after the traffic size increases above the upper backup load sharing threshold.
Null	State other than the above three. At this time, the value for the loadstate field is null.

standby bandwidth

Syntax **standby bandwidth** *size*

undo standby bandwidth

View Interface view

Parameter *size*: Specifies the main interface bandwidth used for setting the thresholds, in the range 0 to 4000000 kbps.

Description Use the **standby bandwidth** command to configure the bandwidth available for transmission on the main interface.

Use the **undo standby bandwidth** command to restore the default.

By default, the available bandwidth used for setting the thresholds is 0 kbps.

Note that:

Use this command after backup interfaces are specified.

- If the available bandwidth used for setting the thresholds is 0kbps (the default value), the backup center automatically obtains the available bandwidth provided by the system to set the thresholds. If the backup center fails to obtain the physical bandwidth, it would prompt you to reconfigure.
- If the available bandwidth configured for setting the thresholds exceeds the physical bandwidth on the interface, the load balancing does not take effect.

Related command: **standby interface**

Example # Configure the available bandwidth used for setting the thresholds on the main interface Serial 2/0 for load sharing to 10000 kbps.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby bandwidth 10000
```

standby interface

Syntax **standby interface** *interface-type interface-number* [*priority*]

undo standby interface *interface-type interface-number*

View Interface view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

priority: Specifies the priority of the backup interface, in the range 0 to 255. The greater the value, the higher the priority. The default is 0.

Description Use the **standby interface** command to specify a backup interface for the current interface.

Use the **undo standby interface** command to remove the specified backup interface.

By default, no backup interface is specified.

Note that:

This command and the **standby interface** command cannot be configured at the same time. That is, if you have configured the **standby interface** command on

the main interface, you cannot configure the **standby track** command on both the main interface and its backup interface; if you have associated an interface with a Track object, you cannot configure the interface as the main interface or a backup interface.

Related commands: **standby track**.

Example # Specify interface Serial 2/1 to back up interface Serial 2/0, and assign it the priority of 50.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby interface serial 2/1 50
```

standby threshold

Syntax **standby threshold** *enable-threshold disable-threshold*

undo standby threshold

View Interface view

Parameter *enable-threshold*: Specifies upper value of the load sharing threshold. It indicates the percentage of the available main-interface bandwidth that the traffic load must exceed for the backup interface to come up for load sharing. It ranges from 1 to 99.

disable-threshold: Specifies lower value of the load sharing threshold. It indicates the percentage of the available main-interface bandwidth that the traffic load must be less than for the backup interface in load sharing to shut down. It ranges from 1 to 99. The disable-threshold must be smaller than the enable-threshold.

Description Use the **standby threshold** command to configure load sharing thresholds.

Use the **undo standby threshold** command to remove the configuration.

By default, load sharing threshold is disabled.

The following is how backup/load sharing works:

- When the traffic on the main interface increases above the enable-threshold, the backup center brings up the highest-priority backup interface, and then other backup interfaces in decreasing priority order depending on traffic size.
- When the traffic on the main interface decreases below the disable-threshold, the backup center shuts down the lowest-priority backup interface first and then other participant backup interfaces in increasing priority order depending on traffic size.

Note that:

- The value of the *enable-threshold* must be bigger than that of the *disable-threshold.*
- If a backup interface has been started, the execution of the **undo standby threshold** command shuts down all backup interfaces.
- Use this command on main interfaces.
- Use this command after backup interfaces are specified.

Related command: **standby interface** and **standby bandwidth**.

Example # Configure the enable-threshold of load sharing on interface Serial 2/0 to 80 and the disable-threshold to 50.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby threshold 80 50
```

standby timer delay

Syntax **standby timer delay** *enable-delay disable-delay*

undo standby timer delay

View Interface view

Parameter *enable-delay*: Specifies failover delay, or the delay for the interface to switch its state from main to standby. It ranges from 0 to 65535 seconds.

disable-delay: Fallback delay, or the delay for the interface to switch from backup to main. It ranges from 0 to 65535 seconds.

Description Use the **standby timer delay** command to set failover and fallback delays on the interface.

Use the **undo standby timer delay** command to restore the default.

By default, failover and fallback delays on the main and backup interfaces are both 0, indicating immediate switch without any delay.

Note that this command can be executed after backup interfaces are specified.

Related command: **standby interface**.

Example # Configure interface Serial 2/1 to use interface Serial 2/0 for backup, and to experience 10 seconds of delay before failover or fallback.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby interface serial 2/1
[Sysname-Serial2/0] standby timer delay 10 10
```

standby timer flow-check

Syntax **standby timer flow-check** *interval*

undo standby timer flow-check

View Interface view

Parameter *interval*: Specifies flow check interval, in the range 30 to 600 seconds.

Description Use the **standby timer flow-check** command to configure the interval for checking the traffic size on the main interface.

Use the **undo standby timer flow-check** command to restore the default.

By default, the interval for checking the traffic size on the main interface is 30 seconds.

Note that this command can be executed after backup interfaces are specified.

Related command: **standby interface**.

Example # Configure load sharing, backup bandwidth and flow check interval on interface Serial 2/0 to 60 seconds.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby timer flow-check 60
```

standby track

Syntax **standby track** *track-entry-number*

undo standby track

View Interface view

Parameters *track-entry-number*: Specifies a Track object to be monitored by its number, in the range 1 to 1024.

Description Use the **standby track** command to configure the association between an interface and a Track object.

Use the **undo standby track** command to remove the association.

By default, an interface is not associated with a Track object.

Note that:

- This command and the **standby interface** command cannot be configured at the same time. That is, if you have configured the **standby interface** command on the main interface, you cannot configure the **standby track** command on both the main interface and its backup interface; if you have associated an interface with a Track object, you cannot configure the interface as the main interface or a backup interface.
- One interface can be associated with one Track object. If you execute this command repeatedly on one interface, the new configuration will overwrite the original one.
- You can associate an interface with a nonexistent Track object. The track function can take effect after the Track object is created with the **track** command.

Related commands: **standby interface**, **track** on page 2529.

Support for this command varies with devices.

Examples # Configure interface Serial 2/0 to be associated with Track object 1.

```
<Sysname> system-view
[Sysname] interface serial 2/0
[Sysname-Serial2/0] standby track 1
```

146 IPv4-Based VRRP Configuration Commands

The interfaces that VRRP involves can only be Layer 3 Ethernet interfaces and VLAN interfaces unless otherwise specified.

display vrrp

Syntax **display vrrp** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter **verbose:** Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp** command to display the state information of VRRP.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

Example # Display brief information about all standby groups on the device before a virtual VRRP standby group is created.

```
<Sysname> display vrrp
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 The total number of the virtual outers: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type       IP
 ------------------------------------------------------------------------
 Eth1/0              1    Master      100     1       NONE     10.10.10.2
```

Display detailed information about all standby groups on the device.

```
<Sysname> display vrrp verbose
 IPv4 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Interface       : Ethernet1/0
 VRID            : 1                    Adver. Timer    : 1
 Admin Status    : UP                   State           : Master
 Config Pri      : 100                  Run Pri         : 100
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Ethernet1/1          Pri Reduced     : 10
 Track Object    : 1                    Pri Reduced     : 10
 Virtual IP      : 10.10.10.2
 Virtual MAC     : 0000-5e00-0101
 Master IP       : 10.10.10.1
```

Table 588 Description on the fields of the display vrrp command

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IP address of the standby group
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Adver. Timer	VRRP advertisement interval
Admin Status	Administrative state: UP or DOWN
State	Status of the router in the standby group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp vrid track interface** command.
Track Object	The object to be tracked. It is displayed only after the execution of the **vrrp vrid track** command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the **vrrp vrid track** command.
Virtual IP	Virtual IP addresses of the standby group
Virtual MAC	Virtual MAC address corresponding to the virtual IP address of the standby group. It is displayed only when the router is in the state of master.
Master IP	Primary IP address of the interface to which the router in the state of master belongs

display vrrp statistics

Syntax **display vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter **interface** *interface-type interface-number*: Displays VRRP statistics of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp statistics** command to display statistics about VRRP.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

Example # Display the statistics about all standby groups.

```
<Sysname> display vrrp statistics
 Interface              : Ethernet1/0
 VRID                   : 1
 CheckSum Errors        : 16         Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 IP TTL Errors          : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 1          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 16         Priority Zero Pkts Sent       : 0
Advertise Sent         : 40
 Interface              : Ethernet1/1
 VRID                   : 105
 CheckSum Errors        : 0          Version Errors                : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors : 0
 IP TTL Errors          : 0          Auth Failures                 : 0
 Invalid Auth Type      : 0          Auth Type Mismatch            : 0
 Packet Length Errors   : 0          Address List Errors           : 0
 Become Master          : 0          Priority Zero Pkts Rcvd       : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent       : 0
Advertise Sent         : 30
Global statistics
 CheckSum Errors        : 16
 Version Errors         : 0
 VRID Errors            : 20
```

Table 589 Description on the fields of the display vrrp statistics command

Field	Description
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types

Table 589 Description on the fields of the display vrrp statistics command

Field	Description
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IP address list errors
Become Master	Number of times that the router worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all standby groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp statistics

Syntax **reset vrrp statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameter **interface** *interface-type interface-number*: Clears VRRP statistics of a specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified standby group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **reset vrrp statistics** command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

Example # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp statistics
```

vrrp vrid authentication-mode

Syntax **vrrp vrid** *virtual-router-id* **authentication-mode** { **md5** | **simple** } *key*

undo vrrp vrid *virtual-router-id* **authentication-mode**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

simple: Plain text authentication mode.

md5: Authentication header (AH) authentication using the MD5 algorithm.

key: Authentication key, case sensitive.

- When **simple** authentication applies, the authentication key is in plain text with a length of 1 to 8 characters.
- When **md5** authentication applies, the authentication key is in MD5 ciphertext or in plain text and the length of the key depends on its input format. If the key is input in plain text, its length is 1 to 8 characters, such as 1234567; if the key is input in ciphertext, its length must be 24 characters, such as _(TT8F]Y5SQ=^Q‘MAF4<1!!.

Description Use the **vrrp vrid authentication-mode** command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.

Use the **undo vrrp vrid authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.

Example # Set the authentication mode and authentication key for VRRP standby group 1 on interface Ethernet 1/0 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.1.1.1
```

vrrp method

Syntax **vrrp method** { **real-mac** | **virtual-mac** }

undo vrrp method

View System view

Parameter **real-mac**: Associates the real MAC address of the interface with the virtual IP address of the standby group.

virtual-mac: Associates the virtual MAC address of the router with the virtual IP address of the standby group.

Description Use the **vrrp method** command to set the mappings between the virtual IP addresses and the MAC addresses of the standby groups.

Use the **undo vrrp method** command to restore the default mapping.

By default, the virtual MAC address of the standby group is associated with the virtual IP address.

You must configure the mapping between the virtual IP address and the MAC address before configuring a standby group. Otherwise, your configuration will fail.

Example # Associate the virtual IP address of the standby group with the real MAC address of the routing interface.

```
<Sysname> system-view
[Sysname] vrrp method real-mac
```

vrrp ping-enable

Syntax **vrrp ping-enable**

undo vrrp ping-enable

View System view

Parameter None

Description Use the **vrrp ping-enable** command to enable users to ping the virtual IP addresses of standby groups.

Use the **undo vrrp ping-enable** command to disable the virtual IP addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

Example # Enable users to ping the virtual IP addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ping-enable
```

vrrp un-check ttl

Syntax **vrrp un-check ttl**

undo vrrp un-check ttl

View Interface view

Parameter None

Description Use the **vrrp un-check ttl** command to disable TTL check on VRRP packets.

Use the **undo vrrp un-check ttl** command to enable TTL check on VRRP packets.

By default, TTL check on VRRP packets is enabled.

Example # Disable TTL check on VRRP packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp un-check ttl
```

vrrp vrid preempt-mode

Syntax **vrrp vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View Interface view

Parameter *virtual-router-id*: Virtual router ID or VRRP standby group number, in the range 1 to 255.

timer delay *delay-value*: Sets preemption delay. The *delay-value* argument ranges from 0 to 255 and defaults to 0, in seconds.

Description Use the **vrrp vrid preempt-mode** command to enable preemption on the router and configure its preemption delay in the specified standby group.

Use the **undo vrrp vrid preempt-mode** command to disable preemption on the router in the specified standby group.

Use the **undo vrrp vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

On an instable network, the standby group member in the backup state may not normally receive the packets from the master member due to network congestion,

resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that before executing the command, you need to create a standby group on an interface and configure the virtual IP address of the standby group.

Example # Enable preemption on the router in VRRP standby group 1, and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Vlan-interface2] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Ethernet1/0] vrrp vrid 1 preempt-mode timer delay 5
```

vrrp vrid priority

Syntax **vrrp vrid** *virtual-router-id* **priority** *priority-value*

undo vrrp vrid *virtual-router-id* **priority**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

priority-value: Priority value of the router in the specified standby group, in the range 1 to 254, with a higher number indicating a higher priority.

Description Use the **vrrp vrid priority** command to configure the priority of the router in the specified standby group.

Use the **undo vrrp vrid priority** command to restore the default.

By default, the priority of a router in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- In VRRP, the role that a router plays in a standby group depends on its priority. A higher priority means that the router is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the router is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Example # Set the priority of the router in standby group 1 to 150.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Ethernet1/0] vrrp vrid 1 priority 150
```

vrrp vrid timer advertise

Syntax **vrrp vrid** *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp vrid *virtual-router-id* **timer advertise**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

adver-interval: Interval at which the master in the specified standby group sends VRRP advertisements. It ranges from 1 to 255 seconds.

Description Use the **vrrp vrid timer advertise** command to configure the interval for Master in the specified standby group to send VRRP advertisements.

Use the **undo vrrp vrid timer advertise** command to restore the default.

By default the interval for Master in the specified standby group to send VRRP advertisements is 1 second.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- Routers in the same VRRP standby group must use the same Adver_Timer setting.

Example # Set the master in standby group 1 to send VRRP advertisements at intervals of five seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Ethernet1/0] vrrp vrid 1 timer advertise 5
```

vrrp vrid track

Syntax **vrrp vrid** *virtual-router-id* **track** *track-entry-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-id* **track** [*object-number*]

View Interface view

Parameters *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

track *track-entry-number*: Specifies a Track object to be monitored by its number. *track-entry-number* ranges from 1 to 1024.

reduced *priority-reduced*: Specifies the value by which the priority decreases. *priority-reduced* ranges from 1 to 255 and defaults to 10.

Description Use the **vrrp vrid track** command to specify the Track object to be monitored. When the status of the monitored Track object changes to negative, the priority of the router decreases by a specified value.

Use the **undo vrrp vrid track** command to cancel the specified Track object.

By default, no Track object is specified to be monitored.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- When the router is the IP address owner, you cannot perform the configuration.
- When the status of the monitored Track object turns from negative to positive, the corresponding router restores its priority automatically.
- The Track object specified in this command can be nonexistent. You can use the **vrrp vrid track** command to specify a Track object, and then create the Track object using the **track** command.

For details of the Track object, refer to "Track Configuration Commands" on page 2529.

Examples # Configure to monitor Track object 1 on interface Ethernet 1/0, making the priority of standby group 1 on Ethernet 1/0 decrease by 50 when Track object 1 turns to negative.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Ethernet1/0] vrrp vrid 1 track 1 reduced 50
```

vrrp vrid track interface

Syntax **vrrp vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

interface *interface-type interface-number*: Specifies an interface to be tracked by its type and number.

reduced *priority-reduced*: Specifies the value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

Description Use the **vrrp vrid track interface** command to configure to track the specified interface.

Use the **undo vrrp vrid track interface** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- When the router is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding router restores its priority automatically.
- The interface specified in this command can be a Layer 3 Ethernet interface, a VLAN interface, a synchronous/asynchronous serial interface, an MP-group interface, a dialer interface or a BRI interface. At present, the Layer 2 protocol used by the tracked synchronous/asynchronous serial interfaces should only be PPP protocol; the dialer interface should function as the PPPoE client and operate in the permanent online mode and the BRI interface should work in the dedicated line mode.

Example # On interface Ethernet 1/0, set the interface to be tracked as Serial 2/0, making the priority of standby group 1 on interface Ethernet 1/0 decrement by 50 when Serial 2/0 goes down.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.1.1.1
[Sysname-Ethernet1/0] vrrp vrid 1 track interface serial2/0 reduced 50
```

vrrp vrid virtual-ip

Syntax **vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address*

undo vrrp vrid *virtual-router-id* [**virtual-ip** *virtual-address*]

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

virtual-address: Virtual IP address.

Description Use the **vrrp vrid virtual-ip** command to create a standby group the first time that you add a virtual IP address or add a virtual IP address to it after that.

Use the **undo vrrp vrid** *virtual-router-id* command to remove a standby group.

Use the **undo vrrp vrid** *virtual-router-id* **virtual-ip** *virtual-address* command to remove a virtual IP address from a standby group.

By default, no standby group is created.

Note that:

- The system removes a standby group after you delete all the virtual IP addresses in it.
- The virtual IP address of the standby group cannot be 0.0.0.0, 255.255.255.255, loopback address, non A/B/C address and other illegal IP addresses such as 0.0.0.1.
- Only when the configured virtual IP address and the interface IP address belong to the same segment and are legal host addresses can the standby group operate normally. If the configured virtual IP address and the interface IP address do not belong to the same network segment, or the configured IP address is the network address or network broadcast address of the network segment that the interface IP address belongs to, the state of the standby group is always **initialize** though you can perform the configuration successfully, that is, VRRP does not take effect in this case.

Example # Create standby group 1 and set its virtual IP address to 10.10.10.10.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp vrid 1 virtual-ip 10.10.10.10
```

Add virtual IP address 10.10.10.11 to standby group 1.

```
[Sysname-Ethernet0/2] vrrp vrid 1 virtual-ip 10.10.10.11
```

147

VRRP CONFIGURATION COMMANDS FOR IPV6

display vrrp ipv6

Syntax **display vrrp ipv6** [**verbose**] [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter **verbose:** Displays detailed state information of VRRP.

interface *interface-type interface-number*: Displays VRRP state information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays state information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp ipv6** command to display the state information of VRRP for IPv6.

If you do not specify **verbose**, only the brief state information of VRRP is displayed.

If you specify both interface and standby group, only the state information of the specified standby group is displayed; if you only specify an interface, the state information of all the standby groups on the interface is displayed; if you specify neither, the state information of all the standby groups on the device is displayed.

Example # Display brief information about all VRRP standby groups on the device for IPv6.

```
<Sysname> display vrrp ipv6
 IPv6 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 The total number of the virtual routers: 1
 Interface          VRID  State       Run     Adver.  Auth     Virtual
                                      Pri     Time    Type       IP
 -------------------------------------------------------------------------
 Eth1/0             1    Master      100     100       NONE     FE80::1
```

Display detailed information about all standby groups on the device.

```
<Sysname> display vrrp ipv6 verbose
 IPv6 Standby Information:
 Run Method      : VIRTUAL-MAC
 Virtual IP Ping : Enable
 Interface       : Ethernet1/0
 VRID            : 1                    Adver. Timer    : 100
 Admin Status    : UP                   State           : Master
 Config Pri      : 100                  Run Pri         : 100
 Preempt Mode    : YES                  Delay Time      : 0
 Auth Type       : NONE
 Track IF        : Ethernet1/1          Pri Reduced     : 10
 Virtual IP      : FE80::1
 Virtual MAC     : 0000-5e00-0201
 Master IP       : FE80::20F:E2FF:FE00:1234
```

Table 590 Description on the fields of the display vrrp ipv6 command

Field	Description
Run Method	Current VRRP running mode, real MAC or virtual MAC
Virtual IP Ping	Whether you can ping the virtual IPv6 address
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
Adver. Timer	VRRP advertisement interval in centiseconds
Admin Status	Administrative state: UP or DOWN
State	Status of the router in the standby group, master, backup, or initialize
Config Pri	Configured priority
Run Pri	Running priority
Preempt Mode	Preemption mode
Delay Time	Preemption delay
Auth Type	Authentication type
Track IF	The interface to be tracked. It is displayed only after the execution of the **vrrp ipv6 vrid track** command.
Pri Reduced	The priority value that is reduced when the interface being tracked is down. It is displayed only after the execution of the **vrrp ipv6 vrid track** command.
Virtual IP	Virtual IPv6 addresses of the standby group
Virtual MAC	Virtual MAC address corresponding to the virtual IPv6 address of the standby group. It is displayed only when the router is in the state of master.
Master IP	Primary IPv6 address of the interface to which the router in the state of master belongs

display vrrp ipv6 statistics

Syntax **display vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View Any view

Parameter **interface** *interface-type interface-number*: Displays VRRP statistics information of the specified interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Displays statistics information of the specified VRRP group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **display vrrp ipv6 statistics** command to display statistics about VRRP for IPv6.

If you specify both interface and standby group, only the statistics about the specified standby group are displayed; if you only specify an interface, the statistics about all the standby groups on the interface are displayed; if you specify neither, the statistics about all the standby groups on the device are displayed.

Example # Display the statistics about all standby groups for IPv6.

```
<Sysname> display vrrp ipv6 statistics
 Interface              : Ethernet1/0
 VRID                   : 80
 CheckSum Errors        : 0          Version Errors                 : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors  : 0
 Hop Limit Errors       : 0          Auth Failures                  : 0
 Invalid Auth Type      : 0          Auth Type Mismatch             : 0
 Packet Length Errors   : 0          Address List Errors            : 0
 Become Master          : 1          Priority Zero Pkts Rcvd        : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent        : 0
 Advertise Sent         : 20

 Interface              : Ethernet1/1
 VRID                   : 10
 CheckSum Errors        : 0          Version Errors                 : 0
 Invalid Type Pkts Rcvd : 0          Advertisement Interval Errors  : 0
 Hop Limit Errors       : 0          Auth Failures                  : 0
 Invalid Auth Type      : 0          Auth Type Mismatch             : 0
 Packet Length Errors   : 0          Address List Errors            : 0
 Become Master          : 1          Priority Zero Pkts Rcvd        : 0
 Advertise Rcvd         : 0          Priority Zero Pkts Sent        : 0
 Advertise Sent         : 30

 Global statistics
 CheckSum Errors        : 0
 Version Errors         : 0
 VRID Errors            : 1439
```

Table 591 Description on the fields of the display vrrp ipv6 statistics command

Field	Description
Interface	Interface to which the standby group belongs
VRID	Number of the standby group
CheckSum Errors	Number of packets with checksum errors
Version Errors	Number of packets with version errors
Invalid Type Pkts Rcvd	Number of packets with incorrect packet type
Advertisement Interval Errors	Number of packets with advertisement interval errors
IP TTL Errors	Number of packets with TTL errors
Auth Failures	Number of packets with authentication failures

Table 591 Description on the fields of the display vrrp ipv6 statistics command

Field	Description
Invalid Auth Type	Number of packets with authentication failures due to invalid authentication types
Auth Type Mismatch	Number of packets with authentication failures due to mismatching authentication types
Packet Length Errors	Number of packets with VRRP packet length errors
Address List Errors	Number of packets with virtual IPv6 address list errors
Become Master	Number of times that the router worked as the master
Priority Zero Pkts Rcvd	Number of received advertisements with the priority of 0
Advertise Rcvd	Number of received advertisements
Advertise Sent	Number of advertisements sent
Global statistics	Statistics about all standby groups
CheckSum Errors	Total number of packets with checksum errors
Version Errors	Total number of packets with version errors
VRID Errors	Total number of packets with VRID errors

reset vrrp ipv6 statistics

Syntax **reset vrrp ipv6 statistics** [**interface** *interface-type interface-number* [**vrid** *virtual-router-id*]]

View User view

Parameter **interface** *interface-type interface-number*: Clears VRRP statistics of a specific interface. *interface-type interface-number* specifies an interface by its type and number.

vrid *virtual-router-id*: Clears VRRP statistics of the specified standby group. *virtual-router-id* specifies a standby group by its group number, in the range 1 to 255.

Description Use the **reset vrrp ipv6 statistics** command to clear VRRP statistics.

If you specify both the interface and standby group, the statistics about the specified standby group on the specified interface are cleared; if you specify only the interface, the statistics about all the standby groups on the interface are cleared; if you specify neither, the statistics about all the standby groups on the device are cleared.

Example # Clear the statistics about all the standby groups on the device.

```
<Sysname> reset vrrp ipv6 statistics
```

vrrp ipv6 method

Syntax **vrrp ipv6 method** { **real-mac** | **virtual-mac** }

undo vrrp ipv6 method

View System view

Parameter **real-mac**: Associates the real MAC address of the interface with the virtual IPv6 address of the standby group.

virtual-mac: Associates the virtual MAC address with the virtual IPv6 address.

Description Use the **vrrp ipv6 method** command to set the mappings between the virtual IPv6 addresses and the MAC addresses of the standby groups.

Use the **undo vrrp ipv6 method** command to restore the default mapping.

By default, the virtual IPv6 address of the standby group is associated with MAC address.

Configure the mapping between the virtual IPv6 address and the MAC address before configuring a standby group. Otherwise, your configuration will fail.

Example # Associate the virtual IP address of the standby group with the real MAC address of the routing interface.

```
<Sysname> system-view
[Sysname] vrrp ipv6 method real-mac
```

vrrp ipv6 ping-enable

Syntax **vrrp ipv6 ping-enable**

undo vrrp ipv6 ping-enable

View System view

Parameter None

Description Use the **vrrp ipv6 ping-enable** command to enable users to ping the virtual IPv6 addresses of standby groups.

Use the **undo vrrp ipv6 ping-enable** command to disable the virtual IPv6 addresses of standby groups from being pinged.

By default, the virtual IP addresses of standby groups can be pinged.

Perform this configuration before configuring a standby group.

Example # Enable users to ping the virtual IPv6 addresses of standby groups.

```
<Sysname> system-view
[Sysname] vrrp ipv6 ping-enable
```

vrrp ipv6 vrid authentication-mode

Syntax **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key*

undo vrrp ipv6 vrid *virtual-router-id* **authentication-mode**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

simple: Sets the authentication mode to plain text authentication.

key: Authentication key of 1 to 8 case-sensitive characters in plain text.

Description Use the **vrrp ipv6 vrid** *virtual-router-id* **authentication-mode simple** *key* command to configure authentication mode and authentication key for the VRRP standby groups to send and receive VRRP packets.

Use the **undo vrrp ipv6 vrid** *virtual-router-id* **authentication-mode** command to restore the default.

By default, authentication is disabled.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IP address of the standby group.
- You may configure different authentication types and authentication keys for the standby groups on an interface. However, the members of the same standby group must use the same authentication mode and authentication key.

Example # Set the authentication mode and authentication key for VRRP standby group 10 on interface Ethernet 1/0 to send and receive VRRP packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp ipv6 vrid 10 virtual-ip fe80::2 link-local
[Sysname-Ethernet1/0] vrrp ipv6 vrid 10 authentication-mode simple Sysname
```

vrrp ipv6 vrid preempt-mode

Syntax **vrrp ipv6 vrid** *virtual-router-id* **preempt-mode** [**timer delay** *delay-value*]

undo vrrp ipv6 vrid *virtual-router-id* **preempt-mode** [**timer delay**]

View Interface view

Parameter *virtual-router-id*: Virtual router ID or VRRP standby group number, in the range 1 to 255.

timer delay *delay-value*: Sets preemption delay. The *delay-value* argument ranges from 0 to 255 and defaults to 0, in seconds.

Description Use the **vrrp ipv6 vrid preempt-mode** command to configure preemption on the router and configure its preemption delay in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode** command to disable preemption on the router in the specified standby group.

Use the **undo vrrp ipv6 vrid preempt-mode timer delay** command to restore the default preemption delay, that is, zero seconds.

The default mode is immediate preemption without delay.

If you set the router in the standby group to work in non-preemption mode, the delay period changes to zero seconds automatically.

On an instable network, the standby group member in the backup state may not normally receive the packets from the master member due to network congestion, resulting in frequent master/backup state transition of the standby group members. Preemption delay is introduced to solve this problem. With a preemption delay set, if the backup member does not receive the packet from the master member duly, it waits for a period to see whether it can receive any packet from the master. If the specified period elapses but it still receives no packet from the master, it becomes the master.

Note that before executing the command, you need to create a standby group on an interface and configure the virtual IPv6 address of the standby group.

Example # Enable preemption on the router in VRRP standby group 80 and set the preemption delay to five seconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp ipv6 vrid 80 virtual-ip fe80::2 link-local
[Sysname-Ethernet1/0] vrrp ipv6 vrid 80 preempt-mode timer delay 5
```

vrrp ipv6 vrid priority

Syntax **vrrp ipv6 vrid** *virtual-router-id* **priority** *priority-value*

undo vrrp ipv6 vrid *virtual-router-id* **priority**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

priority-value: Priority value of the router in the specified standby group, in the range 1 to 254, with a higher number indicating a higher priority.

Description Use the **vrrp ipv6 vrid priority** command to configure the priority of the router in the specified standby group.

Use the **undo vrrp ipv6 vrid priority** command to restore the default.

By default, the priority of a router in a standby group is 100.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- In VRRP, the role that a router plays in a standby group depends on its priority. A higher priority means that the router is more likely to become the master. Note that priority 0 is reserved for special use and 255 for the IP address owner.
- If the router is the IP address owner, its priority is always 255. Therefore, it will be the master so long as it is functioning normally.

Example # Set the priority of the router in standby group 1 to 150.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 priority 150
```

vrrp ipv6 vrid timer advertise

Syntax **vrrp ipv6 vrid** *virtual-router-id* **timer advertise** *adver-interval*

undo vrrp ipv6 vrid *virtual-router-id* **timer advertise**

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

adver-interval: Interval at which the master in the specified standby group sends VRRP advertisements. It ranges from 100 to 4095 centiseconds.

Description Use the **vrrp ipv6 vrid timer advertise** command to configure the Adver_Timer of the specified standby group.

Use the **undo vrrp ipv6 vrid timer advertise** command to restore the default.

By default the Adver_Timer is 100 centiseconds.

The Adver_Timer controls the interval at which the master sends VRRP packets.

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- Routers in the same VRRP standby group must use the same Adver_Timer setting.

Example # Set the master in standby group 1 to send VRRP advertisements at intervals of 500 centiseconds.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
```

```
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 timer advertise 500
```

vrrp ipv6 vrid track

Syntax **vrrp ipv6 vrid** *virtual-router-id* **track interface** *interface-type interface-number* [**reduced** *priority-reduced*]

undo vrrp ipv6 vrid *virtual-router-id* **track** [**interface** *interface-type interface-number*]

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

interface *interface-type interface-number*: Specifies an interface by its type and number.

reduced *priority-reduced*: Specifies the value by which the priority decrements. *priority-reduced* ranges from 1 to 255 and defaults to 10.

Description Use the **vrrp ipv6 vrid track** command to configure to track the specified interface.

Use the **undo vrrp ipv6 vrid track** command to disable tracking the specified interface.

By default, no interface is being tracked.

Note that:

- Before executing the command, create a standby group on an interface and configure the virtual IPv6 address of the standby group.
- When the router is the owner of the IP address, you cannot perform the configuration.
- When the status of the tracked interface turns from down to up, the corresponding router restores its priority automatically.
- The interface specified in this command can be a Layer 3 Ethernet interface, a VLAN interface, or a synchronous/asynchronous serial interface. At present, the layer 2 protocol used by the tracked synchronous/asynchronous serial interfaces can only be PPP protocol.

Example # On interface Ethernet 1/0, set the interface to be tracked as Serial 2/0, making the priority of standby group 1 on interface Ethernet 1/0 decrement by 50 when Serial 2/0 goes down.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 virtual-ip fe80::2 link-local
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 track interface serial 2/0 reduced 50
```

vrrp ipv6 vrid virtual-ip

Syntax **vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**]

undo vrrp ipv6 vrid *virtual-router-id* [**virtual-ip** *virtual-address* [**link-local**]]

View Interface view

Parameter *virtual-router-id*: VRRP standby group number, in the range 1 to 255.

virtual-address: Virtual IPv6 address.

link-local: Indicates that the virtual IPv6 address of the standby group is a link local address.

Description Use the **vrrp ipv6 vrid virtual-ip link-local** command to create a standby group and assign the first virtual IPv6 address to the specified standby group. The first virtual IPv6 address assigned to a standby group must be a link local address and only one such address is allowed in a standby group.

Use the **vrrp ipv6 vrid virtual-ip** command to add a virtual IPv6 address to a standby group.

Use the **undo vrrp ipv6 vrid** command to remove a standby group.

Use the **undo vrrp ipv6 vrid** *virtual-router-id* **virtual-ip** *virtual-address* [**link-local**] command to remove a virtual IPv6 address from a standby group.

After you remove all virtual IPv6 addresses, the standby group is automatically removed. Note that the first address assigned to the group must be removed the last.

By default, no standby group is created.

Example # Create standby group 1, and configure its virtual IPv6 address as fe80::10.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 virtual-ip fe80::10 link-local
```

Configure the virtual IPv6 address of standby group 1 as 1::10.

```
[Sysname-Ethernet1/0] vrrp ipv6 vrid 1 virtual-ip 1::10
```

148 DEVICE MANAGEMENT COMMANDS

There are many types of storage media such as Flash, compact Flash (CF), universal serial bus (USB), and hard disk. Different devices support different types of storage device. CF card is exemplified in this document.

File names in this document comply with the following rules

- *Path + file name (namely, a full file name): File on a specified path. A full file name consists of 1 to 135 characters.*
- *File name" (namely, only a file name without a path): File on the current working path. The file name without a path consists of 1 to 91 characters.*

boot-loader

Syntax **boot-loader file** *file-url* [**slot** *slot-number*] { **main** | **backup** }

View User view

Parameter **file** *file-url*: Specifies a file name, a string of 1 to 64 characters.

slot *slot-number*: Specifies the slot number of a card. The value range varies with devices.

main: Specifies a file as a primary boot file.

backup: Specifies a file as a secondary boot file.

Description Use the **boot-loader** command to specify a boot file on a card.

By default, the boot file is specified as a primary boot file.

A primary boot file is used to boot a device and a secondary boot file is used to boot a device only when a primary boot file is unavailable.

Related command: **display boot-loader**.

Example # Specify the primary boot file of the interface card in slot 2 on a device as plat.bin.

```
<Sysname> boot-loader file plat.bin main
  This command will set boot file, Continue? [Y/N]:y
  The specified file will be used as the main boot file at the next reboot!
```

bootrom

Syntax **bootrom** { **backup** | **read** | **restore** | **update file** *file-url* } [**slot** *slot-number-list*] [**all** | **part**]

View User view

Parameter **read**: Reads Boot ROM.

restore: Restores Boot ROM.

backup: Backs up Boot ROM.

update file *file-url*: Upgrades Boot ROM. *file-url* represents name of the file to be upgraded.

slot *slot-number-list*: Specifies a list of slot numbers of cards, in the format of { *slot-number* [**to** *slot-number*] }&<1-7>. The *slot-number* argument represents the slot number of a card and the value range varies with devices. &<1-7> indicates that you can specify up to seven lists of slot numbers.

all: Operates all contents of Boot ROM.

part: Operates only the extension part of Boot ROM (Boot ROM includes the basic part and the extension part).

Description Use the **bootrom** command to read, restore, back up, or upgrade the Boot ROM program on a card or a device.

If the arguments **all** and **part** are not specified, all contents of the Boot ROM program are operated.

*If the device does not support the Boot ROM extension, the command does not support the **read**, **restore**, **backup**, **all** and **part** keywords.*

Example # Use the a.bin file to upgrade the Boot ROM file on the interface card in slot 1 of a device.

```
<Sysname> bootrom update file a.bin slot 1
  This command will update BootRom file on the specified card(s), Continue?[
Y/N]:y
  Updating BootRom, please wait...

 User 0 update Bootrom on card 1 of board 0 with a.btm success,type is all
```

buzzer enable

Syntax **buzzer enable**

undo buzzer enable

View System view

Parameter None

Description Use the **buzzer enable** command to enable the alarm buzzer function.

Use the **undo buzzer enable** command to disable the alarm buzzer function.

By default, the alarm buzzer function is enabled.

This command is applicable on MSR 50 series routers only.

Example # Enable the temperature alarm buzzer.

```
<Sysname> system-view
[Sysname] buzzer enable
```

display boot-loader

Syntax **display boot-loader** [**slot** *slot-number*]

View Any view

Parameter **slot** *slot-number*: Displays startup file information of the specified card, where *slot-number* represents the slot number of a card. The value range varies with devices.

Description Use the **display boot-loader** command to display the path, name, and primary/secondary attribute of a BootROM file on a card or a device.

Related command: **boot-loader**.

Example # Display the file adopted for the current and next boot of a device (The prompt information of this command varies with devices).

```
<Sysname> display boot-loader
 The boot file used this time:flash:/current.app attr:Maincf:/main.b
in attribute: main
 The boot file be used next time:flash:/main.app attr:Maincf:/main.b
in attribute: main
 The boot file be used next time:flashcf:/backup.app attr:Backupbin
attribute: backup
 The boot file used next time:cf:/secure.bin attribute: secure
```

Table 592 Description on fields on the display boot-loader command

Field	Description
The boot file used this time	File used for the current boot of the device.
attribute	Attributes of a boot file: main (primary)/backup (secondary)/secure (security).
The boot file used next time	Boot file used for the next boot of the device.

display cpu-usage

Syntax **display cpu-usage** [**task**] [*number* [*offset*] [**verbose**] [**from-device**]]

View Any view

Parameter **task**: Displays CPU usage of each task.

number: Number of CPU usage statistics records to be displayed.

offset: Offset between the serial number of the first CPU usage statistics record to be displayed and that of the last CPU usage record to be displayed.

verbose: Specifies to display detailed information of CPU usage statistics.

slave: Specifies to display the statistics of the CPU usage of a standby card.

slot *slot-number*: Specifies to display the statistics of the CPU usage of a card. *slot-number* specifies the slot number of a card. The value range varies with devices.

from-device: Displays external storage devices such as Flash and hard disk. The device currently does not support the **from-device** keyword.

Description Use the **display cpu-usage** command to display the CPU usage statistics.

The system takes statistics of CPU usage at intervals (usually every 60 seconds) and saves the statistical results in the history record area. The maximum number of records that can be saved depends on the device model. **display cpu-usage** *number* indicates the system displays *number* records from the newest (last) record. **display cpu-usage** *number offset* indicates the system displays *number* records from the last but *offset*+1 record.

Equivalent to the **display cpu-usage 1 0 verbose** command, the **display cpu-usage** command displays detailed information of the last CPU usage statistics record.

Example # Display the current CPU usage statistics.

```
<Sysname> display cpu-usage
Slot 4 CPU usage:
     14% in last 5 seconds
     12% in last 1 minute
      8% in last 5 minutes
```

Display detailed information of the last CPU usage statistics record of the current tasks.

```
<Sysname> system-view
[Sysname] display cpu-usage task
===== Current CPU usage info =====
CPU Usage Stat. Cycle: 41 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2006-07-10  11:02:20
```

```
CPU Usage Stat. Tick : 0x1da0(CPU Tick High) 0x62a5077f(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x3d5b5ad1(CPU Tick Low)

TaskName        CPU        Runtime(CPU Tick High/CPU Tick Low)
b2X0             0%               0/   ce77f
VIDL            97%               0/3bc6e650
TICK             0%               0/  23ec62
STMR             0%               0/    ad24
DrTF             0%               0/   28b6b
DrTm             0%               0/   18a28
bCN0             0%               0/   d840e
...omitted...
```

Display the last fifth and sixth records of the CPU usage statistics history.

```
<Sysname> display cpu-usage 2 4
===== CPU usage info (no:  0  idx: 58) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2006-07-10  10:56:55
CPU Usage Stat. Tick : 0x1d9d(CPU Tick High) 0x3a659a70(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x95030517(CPU Tick Low)

===== CPU usage info (no:  1  idx: 57) =====
CPU Usage Stat. Cycle: 60 (Second)
CPU Usage            : 3%
CPU Usage Stat. Time : 2006-07-10  10:55:55
CPU Usage Stat. Tick : 0x1d9c(CPU Tick High) 0xa50e5351(CPU Tick Low)
Actual Stat. Cycle   : 0x0(CPU Tick High) 0x950906af(CPU Tick Low)
```

Table 593 Description on fields of the display boot-loader command

Field	Description
CPU usage info (no: idx:)	Information of CPU usage records (no: The (no+1)th record is currently displayed. no numbers from 0, a smaller number equals a newer record. idx: index of the current record in the history record table). If only the information of the current record is displayed, no and idx are not displayed.
CPU Usage Stat. Cycle	CPU usage measurement period in seconds
CPU Usage	CPU usage in percentage
CPU Usage Stat. Time	CPU usage statistics time in seconds
CPU Usage Stat. Tick	System runtime in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits.
Actual Stat. Cycle	Actual CPU usage measurement period in ticks, represented by a 64-bit hexadecimal. CPU Tick High represents the most significant 32 bits and the CPU Tick Low the least significant 32 bits. Owing to the precision of less than one second, the actual measurement periods of different CPU usage records may differ slightly.
TaskName	Task name
CPU	CPU usage of the current task
Runtime(CPU Tick High/CPU Tick Low)	Running time of the current task

display device

Syntax **display device** [**cf-card** | **usb**] [**slot** *slot-number* | **verbose**]

View Any view

Parameter **cf-card**: Displays information of a compact Flash (CF).

usb: Displays information of a universal serial bus (USB).

slot *slot-number*: Displays detailed information of the specified card. The *slot-number* argument represents the slot number of a card and the value range varies with devices.

verbose: Displays detailed information.

Description Use the **display device** command to display information about storage media such as card, CF, USB, VCPM, VPM and DSP.

Example # Display brief information of cards on a device. (The displayed information varies with devices.)

```
<Sysname> display device
Slot No.   Board Type         Status    Max Ports
 0         AR49-45 RPU Board  Normal       4
 6         DFIC-24FSW         Normal      26
 11        FIX-SNDE           Normal       1
```

Display detailed information of cards on a device. (The displayed information varies with devices.)

```
<Sysname> display device verbose
 Slot No.  Board Type         Status    Max Ports
 0         AR49-45 RPU Board  Normal       4
 6         DFIC-24FSW         Normal      26
 11        FIX-SNDE           Normal       1

 Slot 0
  Status:   Normal
  Type:     AR49-45 RPU Board
  Hardware:  3.0
  Driver:    1.0
  CPLD:     131.0
  VCPM:     Normal   [PCB VER: 3.0  CPLD VER: 1.0  FPGA VER: 2.0]
  VPM0:     Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
            DSP 0:   Normal
            DSP 1:   Normal
            DSP 2:   Normal
            DSP 3:   Normal
  VPM1:     Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
            DSP 0:   Normal
            DSP 1:   Normal
            DSP 2:   Normal
            DSP 3:   Normal
  VPM2:     Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
            DSP 0:   Normal
            DSP 1:   Normal
            DSP 2:   Normal
            DSP 3:   Normal
  VPM3:     Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
```

```
            DSP 0:   Normal
            DSP 1:   Normal
            DSP 2:   Normal
            DSP 3:   Normal
Slot 1
  Status:   Normal
  Type:     SIC-2FXS
  Hardware:  2.2
  Driver:    2.0
  CPLD:      2.0
  DSP:       Normal[DSP VER: 2.0]

Slot 5
  Status:   Normal
  Type:     FIC-2VE1
  Hardware:  3.0
  Driver:    2.0
  CPLD:      1.0
  FDSP:      Normal  [DSP VER: 2.0]
  VCPMA:     Normal   [PCB VER: 3.0  CPLD VER: 1.0  FPGA VER: 2.0]
  VPM0:      Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
             DSP 0:   Normal
             DSP 1:   Normal
             DSP 2:   Normal
             DSP 3:   Normal
  VPM1:      Normal   [PCB VER: 2.0  CPLD VER: 2.0  DSP  VER: 2.0]
             DSP 0:   Normal
             DSP 1:   Normal
             DSP 2:   Normal
             DSP 3:   Normal

 Slot 6
  Status:   Normal
  Type:     DFIC-24FSW
  Hardware:  2.0
  Driver:    1.0
  CPLD:      1.0

 Slot 11
  Status:   Normal
  Type:     FIX-SNDE
  Hardware:  3.0
  Driver:    2.0
  CPLD:     131.0
```

Table 594 Description on fields on the display device command

Field	Description
Slot No.	Slot number of a card
Board Type	Hardware type of a card
Status	Card status
Maximum Ports	Maximum number of physical ports that a card supports
Type	Type of the current card
Hardware	Hardware version of the current card
Driver	Driver version of the current card
CPLD	CPLD version of the current card

Table 594 Description on fields on the display device command

Field	Description
FDSP	DSP status (FDSP version) of the current card
VCPM	VCPM status (PCB, CPLD, FPGA version of VCPM) of the current main board
VCPMA	VCPM status (PCB, CPLD, FPGA version of VCPM) of the current interface card
VPMx	VPM status (PCB, CPLD, DSP version of VPM) of the current card
DSP	DSP status (DSP version) of the current card

VCPM, VCPMA, VPM, FDSP and DSP status includes:

- Normal
- Abnormal
- Reset

display device manuinfo

Syntax **display device manuinfo** [**slot** *slot-number*]

View Any view

Parameter **slot** *slot-number*: Displays detailed information of the specified card. The *slot-number* argument represents the slot number of a card and the value range varies with devices.

Description Use the **display device manuinfo** command to display manufacture information about the device.

Currently, only the cards in the following table support manufacture information display.

Table 595 Cards that support manufacture information display

SIC	MIM	FIC	ESM
SIC-1GEC	MIM-1VE1	FIC-1VE1	ESM-ANDE
SIC-4FSW	MIM-1VT1	FIC-1VT1	ESM-SNDE
DSIC-9FSW	MIM-2VE1	FIC-2VE1	
SIC-1VE1	MIM-2VT1	FIC-2VT1	
SIC-1VT1	MIM-16FSW	FIC-16FSW	
SIC-4FSW-POE	MIM-OAP	DFIC-24FSW	
DSIC-9FSW-POE	MIM-OAP-A	FIC-OAP	
SIC-1BS-V2	MIM-ASM	FIC-ASM	
SIC-2BS-V2	MIM-OAP-B	FIC-OAP-A	
SIC-1BU-V2	MIM-16FSW-POE	FIC-16FSW-POE	
SIC-2BU-V2		DFIC-24FSW-POE	
SIC-1BSV		FIC-24FXS	

Table 595 Cards that support manufacture information display

SIC	MIM	FIC	ESM
SIC-2BSV		DFIC-24O24S	

Example # Display manufacturing information of a device.

```
<Sysname> display device manuinfo
slot 0
DEVICE_NAME:          : NONE
DEVICE_SERIAL_NUMBER  : NONE
MAC_ADDRESS:          : NONE
MANUFACTURING_DATE    : NONE

VENDOR_NAME           : NONE
```

Table 596 Description on the field of the display device manuinfo command

Field	Description
DEVICE_NAME	Device name
DEVICE_SERIAL_NUMBER	Device serial number
MAC_ADDRESS	MAC address of the device
MANUFACTURING_DATE	Manufacturing date of the device
VENDOR_NAME	Manufacturer name

display environment

Syntax **display environment**

View Any view

Parameter None

Description Use the **display environment** command to display the temperature information, including the current temperature and temperature thresholds of cards.

Use the **display environment cpu** command to display the temperature information of all cards or subcards. The displayed information depends on the device model.

Example # Display the temperature information of cards.

```
<Sysname> display environment
System Temperature information (degree centigrade):
-------------------------------------------------
 Board     Temperature       Lower limit      Upper limit
 0         53                10               70
 1         42                10               70
 2         38                10               70
 3         40                10               70
```

Table 597 Description on fields on the display environment command

Field	Description
System Temperature information (degree centigrade)	Temperature information of system cards (degree centigrade)
Board	Card number
Temperature	Current temperature
Lower limit	Lower limit of temperature
Upper limit	Upper limit of temperature

display fan

Syntax **display fan** [*fan-id*]

View Any view

Parameter *fan-id*: Built-in fan number. The value varies with devices.

Description Use the **display fan** command to display the operating state of built-in fans.

Example # Display the operating state of all fans in a device.

```
<Sysname> display fan
 Fan  1 State: Normal
 Fan  2 State: Normal
 Fan  3 State: Normal
```

The above information displays all fans work normally.

display license

Syntax **display license**

View Any view

Parameter None

Description Use the **display license** command to display the software registration information of a device.

Only users at monitor level or a higher level can execute this command.

Example # Display the software registration information of a device.

```
<Sysname> display license
Software license information
-----------------------------------------------
Serial Number: VZa47-6AbBh-gtO9c-K47A0-F79D8-dE84O-tg2j0
```

```
Register Date: 2006-10-10 15:50:28
Trade Code   : 121234A757C06A000693
```

Table 598 Descriptions on the fields of the display license command

Field	Description
Software license information	Software license information of a device
Serial Number	Serial number of a device
Register Date	Register date and time
Trade Code	Trade code (that is, manufacturing serial number)

display memory

Syntax **display memory**

View Any view

Parameter None

Description Use the **display memory** command to display the usage of the memory of a device.

Example # Display the usage of the memory of a device.

```
<Sysname> display memory
System Total Memory(bytes): 431869088
Total Used Memory(bytes): 71963156
Used Rate: 16%
```

Table 599 Description on fields on the display memory command

Field	Description
System Total Memory(bytes)	Total size of the system memory (in bytes)
Total Used Memory(bytes)	Size of the memory used (in bytes)
Used Rate	Percentage of the memory used to the total memory

display power

Syntax **display power** [*power-id*]

View Any view

Parameter *power-id*: Power supply number.

Description Use the **display power** to display the status of the power supply of a device.

Example # Display the status of the power supply of a device. (The displayed information varies with devices).

```
<Sysname> display power
 Power   1 State: Absent
 Power   2 State: Normal
 Power   3 State: Absent
```

The above information indicates that power supply 2 works normally, and power supply 1 and power supply 3 are absent.

display reboot-type

Syntax **display reboot-type** [**slot** *slot-number*]

View Any view

Parameter **slot** *slot-number*: Displays reboot type of the specified card, where *slot-number* represents the slot number of a card. The value range varies with devices.

Description Use the **display reboot-type** command to display the reboot type of a device.

Example # Display the reboot type of the card in slot 2 of the device.

```
<Sysname> display reboot-type slot 2
The rebooting type this time is: Cold
```

The above information indicates that the last reboot type of the device is Cold boot. (If it is displayed as Warm, it indicates the reboot type is ware boot).

display schedule reboot

Syntax **display schedule reboot**

View Any view

Parameter None

Description Use the **display schedule reboot** command to display the device reboot time set by the user.

Related command: **schedule reboot at** and **schedule reboot delay**.

Example # Display the reboot time of a device.

```
<Sysname> display schedule reboot
System will reboot at 16:00:00 2006/03/10 (in 2 hours and 5 minutes).
```

The above information indicates the system will reboot at 16:00:00 on March 10, 2006 (in two hours and five minutes).

license register

Syntax **license register** *serial-number*

View User view

Parameter *serial-number*: Specifies the serial number of a card, in the format of *XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX-XXXXX*, in which X represents a character. The character can be a letter (case sensitive), a number, + or (/).

Description Use the **license register** command to register the software serial number for a device.

The serial number can be obtained by purchasing letter of authorization. To successfully register a serial number, you must enter the serial number in the specified format.

Only users at management level can execute this command.

Example # Register the software serial number of a device.

```
<Sysname> system-view
[Sysname] license register VZa47-6AbBh-gtO9c-K47A0-F79D8-dE84O-tg2j0
Register successfully!
```

reboot

Syntax **reboot** [**slot** *slot-number*]

View User view

Parameter **slot** *slot-number*: Specifies the slot number of a card. The value range varies with devices.

Description Use the **reboot** command to reboot a card or a device.

CAUTION:

- *This command reboots the device, thus resulting in service interruption. Please use it with caution.*
- *If a primary boot file fails or does not exist, the device cannot be rebooted with this command. In this case, you can re-specify a primary boot file to reboot the device, or you can power off the device then power it on and the system automatically uses the secondary boot file to restart the device.*
- *The **slot** keyword is applicable on an MSR 50 series router only.*

Example # Reboot the device.

```
<Sysname> reboot
Start to check configuration with next startup configuration file, please wait
......
  This command will reboot the device. Current configuration will be lost in next
 startup if you continue. Continue? [Y/N]:y
  This will reboot device. Continue? [Y/N]:y
  #Nov 20 12:00:42:698 2006 Sysname COMMONSY/4/REBOOT:
   Reboot device by command.
  %Nov 20 12:00:42:699 2006 Sysname DEV/4/SYSTEM REBOOT:
 System is rebooting now.

Now rebooting, please wait...
```

remove

Syntax **remove slot** *slot-number*

View User view

Parameter **slot** *slot-number*: Specifies the slot number of a card. The value range varies with devices.

Description Use the **remove** command to remove a card.

This command is supported only on MSR 50 series routers.

CAUTION:

- *This command may cause a card unusable, thus resulting in service interruption. Use it with caution.*
- *Use the **remove slot** command to remove a card before hot swapping it; otherwise the device or the card may be broken.*

Example # Remove card 8.

```
<Sysname>remove slot 8
 You can not configure the slot now.
 Please wait...
 You can remove the card now.
```

reset unused porttag

Syntax **reset unused porttag**

View User view

Parameter None

Description Use the **reset unused porttag** command to clear the 16-bit index saved but not used in the current system.

A confirmation is required when you carry out this command. If you fail to make a confirmation within 30 seconds or enter "N" to cancel the operation, the command will not be carried out.

Example # Clear the 16-bit index saved but not used in the current system.

```
<Sysname> reset unused porttag
Current operation will delete all unused port tag(s). Continue? [Y/N]:y
<Sysname>
```

schedule reboot at

Syntax **schedule reboot at** *hh:mm* [*date*]

undo schedule reboot

View User view

Parameter *hh:mm*: Reboot time of a device, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 23, and the value of the *mm* argument ranges from 0 to 59.

date: Reboot date of a device, in the format mm/dd/yyyy (Month/day/year) or in the format yyyy/mm/dd (year/month/day) The yyyy value ranges from 2000 to 2035, the mm value ranges from 1 to 12, and the dd value depends on a specific month.

Description Use the **schedule reboot at** command to enable the scheduled reboot function and specify a specific reboot time and date.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

There are two cases if no specific reboot date is specified:

- When the specified reboot time is later than the current time, the device will be rebooted at the reboot time of the current day.
- When the specified reboot time is earlier than the current time, the device will be rebooted at the reboot time the next day.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

Note that:

- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- The difference between the reboot date and the current date cannot exceed 30 x 24 hours (namely, 30 days).

- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If a date (month/day/year or year/month/day) later than the current date is specified for the **schedule reboot at** command, the device will be rebooted at the reboot time.
- If you use the **clock** command after the **schedule reboot at** command to adjust the system time, the reboot time set by the **schedule reboot at** command will become invalid.

CAUTION: *This command reboots the device in a future time, thus resulting in service interruption. Please use it with caution.*

Example # Configure the device to reboot at 12:00 AM (supposing that the current time is 11:43).

```
<Sysname> schedule reboot at 12:00
Reboot system at 12:00 2006/06/06(in 0 hour(s) and 16 minute(s))
confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled.

```
<Sysname>
%Jun  6 11:43:11:629 2006 Sysname CMD/5/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:43:11 2006/
06/06, and system will reboot at 12:00 2006/06/06.
```

schedule reboot delay

Syntax **schedule reboot delay** { *hh:mm* | *mm* }

undo schedule reboot

View User view

Parameters *hh:mm*: Device reboot wait time, in the format of hh:mm (hours:minutes). The value of the *hh* argument ranges of is 0 to 720, and the value of the *mm* argument ranges from 0 to 59, and the value of the *hh:mm* argument cannot exceed 720:00.

mm: Device reboot wait time in minutes, in the range of 0 to 43,200.

Description Use the **schedule reboot delay** command to enable the scheduled reboot function and set a reboot wait time.

Use the **undo schedule reboot** command to disable the scheduled reboot function.

By default, the scheduled reboot function is disabled.

Note that:

- The reboot wait time can be in the format of hh:mm (hours:minutes) or mm (absolute minutes). The absolute minutes cannot exceed 30 x 24 x 60 minutes, namely, 30 days.
- The precision of the device timer is 1 minute. One minute before the reboot time, the device will prompt "REBOOT IN ONE MINUTE" and will be rebooted in one minute.
- After you execute the above command, the device will prompt you to confirm the configuration. You must enter <Y> or <y> to make the configuration take effect. The original configuration will be overwritten at the same time.
- If you use the **clock** command after the **schedule reboot delay** command to adjust the system time, the reboot wait time set by the **schedule reboot delay** command will become invalid.
- If you are performing file operations when the device is to be rebooted, the system does not execute the command for the sake of security.

CAUTION: *This command reboots the device after the specified delay time, thus resulting in service interruption. Please use it with caution.*

Example # Configure the device to reboot in 88 minutes (supposing the current time is 11:48).

```
<Sysname> schedule reboot delay 88
Reboot system at 13:16 2006/06/06(in 1 hour(s) and 28 minute(s))
confirm? [Y/N]:
```

If you have used the **terminal logging** command to enable the log display function on the terminal before setting a reboot time, the system will automatically display related log information after you enter <y>. By default, the log display function is enabled on the terminal.

```
<Sysname>
%Jun  6 11:48:44:860 2006 Sysname CMD/5/REBOOT:
vty0(192.168.1.54): Set schedule reboot parameters at 11:48:44 2006/
06/06, and system will reboot at 13:16 2006/06/06.
```

temperature-alarm enable

Syntax **temperature-alarm enable**

undo temperature-alarm enable

View System view

Parameter None

Description Use the **temperature-alarm enable** command to enable the temperature alarm function.

Use the **undo temperature-alarm enable** command to disable the temperature alarm function.

By default, the temperature alarm function is enabled.

Example # Enable the temperature alarm function.

```
<Sysname> system-view
[Sysname] temperature-alarm enable
```

temperature-limit

Syntax **temperature-limit** *slot-number lower-value upper-value*

undo temperature-limit *slot-number*

View System view

Parameter *slot-number*: Slot number. The value range varies with devices.

lower-value: Lower temperature limit in Celsius degrees, in the range 0 to 30.

upper-value: Upper temperature limit in Celsius degrees, in the range 40 to 90.

Description Use the **temperature-limit** command to set the temperature alarm threshold on a card.

Use the **undo temperature-limit** command to restore the temperature alarm threshold to the default.

By default, the lower value and the upper value of the temperature alarm threshold is 5 and 60 respectively.

Example # Set the lower temperature limit on card 0 to 10 Celsius degrees and the upper temperature limit to 75 Celsius degrees.

```
<Sysname> system-view
[Sysname] temperature-limit 0 10 75
Setting temperature limit succeeded.
```

149 NQA CLIENT CONFIGURATION COMMANDS

data-fill

Syntax **data-fill** *string*

undo data-fill

View ICMP-echo/UDP-echo/UDP-jitter test type view

Parameter *string*: String of fill characters of a probe packet, in the range 1 to 200. It is case sensitive.

Description Use the **data-fill** command to configure the string of fill characters of a probe packet.

Use the **undo data-fill** command to restore the default.

By default, the string of fill characters of a probe packet is the string corresponding to the ASCII code 00 to 09.

- If the probe packet is smaller than the fill data, the system uses only the first part of the character string to encapsulate the packet.
- If the probe packet is larger than the fill data, the system fills the character string cyclically to encapsulate the packet until it is full.

For example, when the fill data is **abcd** and the size of a probe packet is 3 byte, **abc** is used to fill the packet. When the probe size is 6 byte, **abcdab** is used to fill the packet.

- Because the first five bytes of a probe packet in a UDP-echo test have some specific usage, the configured character string is used to fill the remaining bytes in the probe packet.
- Because the first 68 bytes of a probe packet in UDP-jitter test have some specific usage, the configured character string is used to fill the remaining bytes in the probe packet.

Example # Configure the string of fill characters of an ICMP-echo probe packet as **abcd**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-fill abcd
```

data-size

Syntax **data-size** *size*

undo data-size

View ICMP-echo/UDP-echo/UDP-jitter test type view

Parameter ***size***: Size of a probe packet in bytes, in the range 20 to 8100 for an ICMP-echo or a UDP-echo test and in the range 68 to 8100 for a UDP-jitter test.

Description Use the **data-size** command to configure the size of a probe packet sent, namely, the size of a packet sent (IP header and ICMP header excluded) in a probe.

Use the **undo data-size** command to restore the default.

By default, the size of a probe packet is 100 bytes.

Example # Configure the size of an ICMP-echo probe packet as 80 bytes.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] data-size 80
```

description (any NQA test type view)

Syntax **description** *text*

undo description

View Any NQA test type view

Parameter *text*: Descriptive string of a test group, in the range 1 to 200 characters. It is case sensitive.

Description Use the **description** command to give a brief description of a test group, usually, the test type or test purpose of a test group.

Use the **undo description** command to remove the configured description information.

By default, no descriptive string is available for a test group.

Example # Configure the descriptive string for a test group as **icmp-probe**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] description icmp-probe
```

destination ip

Syntax **destination ip** *ip-address*

undo destination ip

View DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo/UDP-jitter test type view

Parameter *ip-address*: Destination IP address of a test operation.

Description Use the **destination ip** command to configure a destination IP address for a test operation.

Use the **undo destination ip** command to remove the configured destination IP address.

By default, no destination IP address is configured for a test operation.

Example # Configure the destination IP address of an ICMP-echo test operation as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] destination ip 10.1.1.1
```

destination port

Syntax **destination port** *port-number*

undo destination port

View TCP/UDP-echo/UDP-jitter test type view

Parameter *port-number*: Destination port number of a test operation, in the range 1 to 65535.

Description Use the **destination port** command to configure a destination port number for a test operation.

Use the **undo destination port** command to remove the configured destination port number.

By default, no destination port number is configured for a test operation.

Note that you are not recommended to perform a TCP, UDP-echo, or UDP-jitter test on ports from 1 to 1023 (known ports). Otherwise, the NQA test will fail or the corresponding services of this port will be unavailable.

Example # Configure the destination port number of a test operation as 9000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] destination port 9000
```

display nqa

Syntax **display nqa** { **result** | **history** } [*admin-name operation-tag*]

View Any view

Parameter **result**: Displays the results of the last test.

history: Displays the history records of a test.

admin-name: Specifies the name of the administrator who creates NQA operations, a string of 1 to 32 characters. It is case-insensitive.

operation-tag: Specifies the test operation tag, a string of 1 to 32 characters. It is case-insensitive.

Description Use the **display nqa** command to display operation information of an NQA test or tests.

If neither of the test group arguments (*admin-name* and *operation-tag*) is specified, information of all test groups is displayed.

Example # Display the results of the last test.

```
<Sysname> display nqa result administrator jitter
  NQA entry(admin administrator, tag jitter) test results:
    Destination IP address: 192.168.0.81
      Send operation times: 10             Receive response times: 0
      Min/Max/Average round trip time: 0/0/0
      Square-Sum of round trip time: 0
      Last succeeded probe time: 0-00-00 00:00:00.0
    Extend results:
      Packet lost in test: 100%
      Failures due to timeout: 10
      Failures due to disconnect: 0
      Failures due to no connection: 0
      Failures due to sequence error: 0
      Failures due to internal error: 0
      Failures due to other errors: 0
    UDP-jitter results:
     RTT number: 0
      SD max delay: 0                      DS max delay: 0
      Min positive SD: 0                   Min positive DS: 0
      Max positive SD: 0                   Max positive DS: 0
      Positive SD number: 0                Positive DS number: 0
      Positive SD sum: 0                   Positive DS sum: 0
      Positive SD average: 0               Positive DS average: 0
      Positive SD square sum: 0            Positive DS square sum: 0
      Min negative SD: 0                   Min negative DS: 0
      Max negative SD: 0                   Max negative DS: 0
      Negative SD number: 0                Negative DS number: 0
      Negative SD sum: 0                   Negative DS sum: 0
```

```
Negative SD average: 0                Negative DS average: 0
Negative SD square sum: 0             Negative DS square sum: 0
SD lost packet(s): 0                  DS lost packet(s): 0
Lost packet(s) for unknown reason: 10
```

Table 600 Description on the fields of the display nqa result command

Field	Description
Destination IP address	IP address of the destination
Send operation times	Number of probe packets sent
Receive response times	Number of response packets received
Min/Max/Average round trip time	Minimum/maximum/average roundtrip time
Square-Sum of round trip time	Square sum of roundtrip time
Last succeeded probe time	Time when the last probe succeeded in a test
Packet lost in test	Average packet loss ratio
Failures due to timeout	Number of timeout occurrences in a test
Failures due to disconnect	Number of disconnections by the peer
Failures due to no connection	Number of failures to connect with the peer
Failures due to sequence error	Number of failures owing to out-of-sequence packets
Failures due to internal error	Number of failures owing to internal errors
Failures due to other errors	Failures due to other errors
UDP-jitter results	UDP-jitter test results, available only in UDP-jitter tests.
RTT number	Number of response packets received
SD max delay	Maximum delay from the source to the destination
DS max delay	Maximum delay from the destination to the source
Min positive SD	Minimum positive jitter delay from the source to the destination
Min positive DS	Minimum positive jitter delay from the destination to the source
Max positive SD	Maximum positive jitter delay from the source to the destination
Max positive DS	Maximum positive jitter delay from the destination to the source
Positive SD number	Number of positive jitter delays from the source to the destination
Positive DS number	Number of positive jitter delays from the destination to the source
Positive SD sum	Sum of positive jitter delays from the source to the destination
Positive DS sum	Sum of positive jitter delays from the destination to the source
Positive SD average	Average of positive jitter delays from the source to the destination
Positive DS average	Average of positive jitter delays from the destination to the source
Positive SD square sum	Sum of the square of positive jitter delays from the source to the destination

Table 600 Description on the fields of the display nqa result command

Field	Description
Positive DS square sum	Sum of the square of positive jitter delays from the destination to the source
Min negative SD	Minimum absolute value of negative jitter delays from the source to the destination
Min negative DS	Minimum absolute value of negative jitter delays from the destination to the source
Max negative SD	Maximum absolute value of negative jitter delays from the source to the destination
Max negative DS	Maximum absolute value of negative jitter delays from the destination to the source
Negative SD number	Number of negative jitter delays from the source to the destination
Negative DS number	Number of negative jitter delays from the destination to the source
Negative SD sum	Sum of absolute values of negative jitter delays from the source to the destination
Negative DS sum	Sum of absolute values of negative jitter delays from the destination to the source
Negative SD average	Average of negative jitter delays from the source to the destination
Negative DS average	Average of negative jitter delays from the destination to the source
Negative SD square sum	Sum of the square of negative jitter delays from the source to the destination
Negative DS square sum	Sum of the square of negative jitter delays from the destination to the source
SD lost packet(s)	Number of lost packets from the source to the destination
DS lost packet(s)	Number of lost packets from the destination to the source
Lost packet(s) for unknown reason	Number of lost packets for unknown reasons

Display the history records of tests.

```
<Sysname> display nqa history administrator test
  NQA entry(admin administrator, tag test) history record(s):
    Index      Response     Status           Time
    10         329          Succeeded        2007-04-29 20:54:26.5
    9          344          Succeeded        2007-04-29 20:54:26.2
    8          328          Succeeded        2007-04-29 20:54:25.8
    7          328          Succeeded        2007-04-29 20:54:25.5
    6          328          Succeeded        2007-04-29 20:54:25.1
    5          328          Succeeded        2007-04-29 20:54:24.8
    4          328          Succeeded        2007-04-29 20:54:24.5
    3          328          Succeeded        2007-04-29 20:54:24.1
    2          328          Succeeded        2007-04-29 20:54:23.8
    1          328          Succeeded        2007-04-29 20:54:23.4
```

Table 601 Description on the fields of the display nqa history command

Field	Description
Index	History record number

Table 601 Description on the fields of the display nqa history command

Field	Description
Response	Roundtrip delay of a test packet in the case of a successful test, timeout time in the case of timeout, or 0 in the case of a test failure (in milliseconds)
Status	Status value of test results, including: ■ Succeeded ■ Unknown error ■ Internal error ■ Timeout
Time	Time when the test is completed

filename

Syntax **filename** *filename*

undo filename

View FTP test type view

Parameter *filename*: Name of the file transferred between the FTP server and the FTP client, a string of 1 to 200 characters. It is case sensitive.

Description Use the **filename** command to specify a file to be transferred between the FTP server and the FTP client.

Use the **undo filename** command to restore the default.

By default, no file is specified.

Example # Specify the file to be transferred between the FTP server and the FTP client as config.txt.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] filename config.txt
```

frequency

Syntax **frequency** *interval*

undo frequency

View Any NQA test type view

Parameter *interval*: Interval between two consecutive tests, in milliseconds, in the range 0 to 604800000. If the interval is 0, it indicates that only one test is performed.

Description Use the **frequency** command to configure the interval between two consecutive tests for a test group.

Use the **undo frequency** command to restore the default.

By default, the interval between two consecutive tests for a test group is 0 milliseconds, that is, only one test is performed.

After you use the **nqa schedule** command to start an NQA test, one test is started at *interval*.

*If the last test is not completed when the interval specified by the **frequency** command is reached, a new test is not started.*

Example # Configure the interval between two consecutive tests as 1000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] frequency 1000
```

history-records

Syntax **history-records** *number*

undo history-records

View Any NQA test type view

Parameter *number*: Maximum number of history records that can be saved in a test group, in the range 0 to 50.

Description Use the **history-records** command to configure the maximum number of history records that can be saved in a test group.

Use the **undo history-records** command to restore the default.

By default, the maximum number of records that can be saved in a test group is 50.

If the number of history records exceeds the maximum number, the earliest history record for a probe will be discarded.

Example # Configure the maximum number of history records that can be saved in a test group as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin test
```

```
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] history-records 10
```

http-version

Syntax **http-version v1.0**

undo http-version

View HTTP test type view

Parameter **v1.0**: The HTTP version is 1.0 in an HTTP test.

Description Use the **http-version** command to configure the HTTP version used in an HTTP test.

Use the **undo http-version** command to restore the default.

By default, HTTP 1.0 is used in an HTTP test.

Example # Configure the HTTP version as 1.0 in an HTTP test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] http-version v1.0
```

next-hop

Syntax **next-hop** *ip-address*

undo next-hop

View ICMP-echo test type view

Parameter *ip-address*: IP address of the next hop.

Description Use the **next-hop** command to configure the next hop IP address for an IP packet.

Use the **undo next-hop** command to remove the configured next hop IP address.

By default, no next hop IP address is configured.

Example # Configure the next hop IP address as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] next-hop 10.1.1.1
```

nqa

Syntax **nqa entry** *admin-name operation-tag*

undo nqa { **all** | **entry** *admin-name operation-tag* }

View System view

Parameter *admin-name*: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters, with "-" excluded. It is case-insensitive.

operation-tag: Specifies the tag of a test operation, a string of 1 to 32 characters, with "-" excluded. It is case-insensitive.

all: All NQA test groups.

Description Use the **nqa** command to create an NQA test group and enter NQA test group view.

Use the **undo nqa** command to remove the test group.

Note that if the test type has been configured for the test group, you will directly enter NQA test type view when you execute the **nqa** command.

Example # Create an NQA test group whose administrator name is **admin** and whose operation tag is **test** and enter NQA test group view.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test]
```

nqa agent enable

Syntax **nqa agent enable**

undo nqa agent enable

View System view

Parameter None

Description Use the **nqa agent enable** command to enable the NQA client.

Use the **undo nqa agent enable** command to disable the NQA client and stop all the tests being performed.

By default, the NQA client is enabled.

Related command: **nqa server enable**.

Example # Enable the NQA client.

```
<Sysname> system-view
[Sysname] nqa agent enable
```

nqa agent max-concurrent

Syntax **nqa agent max-concurrent** *number*

undo nqa agent max-concurrent

View System view

Parameter *number*: Maximum number of the tests that the NQA client can simultaneously perform, in the range 1 to 50

Description Use the **nqa agent max-concurrent** command to configure the maximum number of tests that the NQA client can simultaneously perform.

Use the **undo nqa agent max-concurrent** command to restore the default.

From the beginning to the end of a test, the NQA test is in the test status; from the end of a test to the beginning of the next test, the NQA test is in the waiting status.

Example # Configure the maximum number of the tests that the NQA client can simultaneously perform as 50.

```
<Sysname> system-view
[Sysname] nqa agent max-concurrent 50
```

nqa schedule

Syntax **nqa schedule** *admin-name operation-tag* **start-time now lifetime forever**

undo nqa schedule *admin-name operation-tag*

View System view

Parameter *admin-name*: Specifies the name of the administrator who creates the NQA test operation, a string of 1 to 32 characters. It is case-insensitive.

operation-tag: Specifies the test operation tag, a string of 1 to 32 characters. It is case-insensitive.

now: Specifies to start the test for a test group immediately.

forever: Specifies that the test is performed for a test group forever.

Description Use the **nqa schedule** command to configure the test start time and test period for a test group.

Use the **undo nqa schedule** command to stop the test for the test group.

Note that a test group is not allowed to enter test group view or test type view after it is scheduled.

Example # Start a test for the test group with the administrator name **admin** and operation tag **test**.

```
<Sysname> system-view
[Sysname] nqa schedule admin test start-time now lifetime forever
```

operation (FTP test type view)

Syntax **operation** { **get** | **put** }

undo operation

View FTP test type view

Parameter **get**: Obtains a file from the FTP server.

put: Transfers a file to the FTP server.

Description Use the **operation** command to configure the FTP operation type.

Use the **undo operation** command to restore the default.

By default, the FTP operation type is **get**.

Example # Configure the FTP operation type as **put**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] operation put
```

operation (HTTP test type view)

Syntax **operation** { **get** | **post** }

undo operation

View HTTP test type view

Parameter **get**: Obtains data from the HTTP server.

post: Transfers data to the HTTP server.

Description Use the **operation** command to configure the HTTP operation type.

Use the **undo operation** command to restore the default.

By default, the HTTP operation type is **get**.

Example # Configure the HTTP operation type as **post**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] operation post
```

operation interface

Syntax **operation interface** *interface-type interface-number*

undo operation interface

View DHCP test type view

Parameter *interface-type interface-number*: Type and number of the interface that is performing a DHCP test.

Description Use the **operation interface** command to specify the interface to perform a DHCP test.

Use the **undo operation interface** command to remove the configured interface to perform the DHCP test.

By default, no interface is specified to perform a DHCP test.

Note that the specified interface must be up; otherwise, the test will fail.

Example # Specify the interface to perform a DHCP test as Ethernet 1/0.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Sysname-nqa-admin-test-dhcp] operation interface ethernet 1/0
```

password (FTP test type view)

Syntax **password** *password*

undo password

View FTP test type view

Parameter *password*: Password used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

Description Use the **password** command to configure a password used to log onto the FTP server.

Use the **undo password** command to remove the configured password.

By default, no password is configured for logging onto the FTP server.

Related command: "username (FTP test type view)" on page 2287, "operation (FTP test type view)" on page 2276.

Example # Configure the password used for logging onto the FTP server as **ftpuser**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] password ftpuser
```

probe count

Syntax **probe count** *times*

undo probe count

View Any NQA test type view

Parameter *times*: Number of probes in a test, in the range 1 to 15.

Description Use the **probe count** command to configure the number of probes in a test.

Use the **undo probe count** command to restore the default.

By default, one probe is performed in a test.

- For a TCP or DLSw test, one probe means one connection;
- For a UDP-jitter test, the number of packets sent in one probe depends on the **probe packet-number** command;
- For an FTP, HTTP or DHCP test, one probe means to carry out a corresponding function;
- For an ICMP-echo or UDP-echo test, one packet is sent in one probe;
- For an SNMP test, three packets are sent in a probe.

If the number of probes in a test is greater than 1, the system sends a second packet after it sends the first packet and receives a response packet. If the system does not receive a response packet, it waits for the test timer to expire before sending a second probe packet. The process is repeated until the specified probes are completed.

Example # Configure the number of probes in an ICMP-echo test as 10.

```
<Sysname> system-view
[Sysname] nqa entry admin-test
[Sysname-nqa-admin-test] type icmp-echo
[Syaname-nqa-admin-test-icmp-echo] probe count 10
```

probe packet-interval

Syntax **probe packet-interval** *packet-interval*

undo probe packet-interval

View UDP-jitter test type view

Parameter *packet-interval*: Interval for consecutive packets sent, in milliseconds, in the range 10 to 1000.

Description Use the **probe packet-interval** command to configure the interval for sending consecutive packets.

Use the **undo probe-interval** command to restore the default.

By default, the interval for sending consecutive packets is 20 milliseconds.

Example # Configure the interval for sending consecutive packets as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-interval 100
```

probe packet-number

Syntax **probe packet-number** *packet-number*

undo probe packet-number

View UDP-jitter test type view

Parameter *packet-number*: Number of consecutive packets sent in a UDP-jitter test, in the range 10 to 1000.

Description Use the **probe packet-number** command to configure the number of consecutive packets sent in a UDP-jitter probe.

Use the **undo probe packet-number** command to restore the default.

By default, the number of consecutive packets in a probe is 10.

Example # Configure the number of consecutive packets in a UDP-jitter probe as 100.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-number 100
```

probe packet-timeout

Syntax **probe packet-timeout** *packet-timeout*

undo probe packet-timeout

View UDP-jitter test type view

Parameter *packet-timeout*: Timeout time for waiting for responses in a UDP-jitter test, in the range 10 to 3600000 milliseconds.

Description Use the **probe packet-timeout** command to configure the timeout time for waiting for responses in a UDP-jitter test.

Use the **undo probe packet-timeout** command to restore the default.

By default, the timeout time in a UDP-jitter test is 3000 milliseconds.

Example # Configure the timeout time for waiting for responses in a UDP-jitter test as 100 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-jitter
[Syaname-nqa-admin-test-udp-jitter] probe packet-timeout 100
```

probe timeout

Syntax **probe timeout** *timeout*

undo probe timeout

View DHCP/DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo test type view

Parameter *timeout*: Timeout time in a probe except UDP-jitter probe, in milliseconds. For an FTP or HTTP probe, the value range is 10 to 86400000; for a DHCP, DLSw, ICMP-echo, SNMP, TCP or UDP-echo probe, the value range is 10 to 3600000.

Description Use the **probe timeout** command to configure the timeout time in a probe.

Use the **undo probe timeout** command to restore the default.

By default, the timeout time is 3000 milliseconds.

Example # Configure the timeout time in a DHCP probe as 10000 milliseconds.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type dhcp
[Syaname-nqa-admin-test-dhcp] probe timeout 10000
```

reaction

Syntax **reaction** *item-num* **checked-element probe-fail threshold-type consecutive** *occurrences* [**action-type** { **none** | **trigger-only** }]

undo reaction *item-num*

View DHCP/DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo test type view

Parameter *item-num*: Number of the collaboration entry, in the range 1 to 10.

checked-element: Type of the monitored element in collaboration. At present, the type of the monitored element can be probe failure only.

probe-fail: The type of the monitored element is probe failure.

threshold-type consecutive: Threshold type is consecutive probe failures.

occurrences: Number of consecutive probe failures, in the range 1 to 16.

action-type: Triggered action type, defaulting to **none**.

none: No actions.

trigger-only: Triggers collaboration between other modules only.

Description Use the **reaction** command to establish a collaboration entry to monitor the probe results of the current test group. If the number of consecutive probe failures reaches the threshold, collaboration with other modules is triggered.

Use the **undo reaction** command to remove the collaboration entry.

By default, no collaboration entries are configured.

Note that you cannot modify the content of a collaboration object using the **reaction** command after the collaboration object is created.

Related command: "track" on page 2529.

Example # Create collaboration object 1. If the number of consecutive probe failures reaches 3, collaboration with other modules is triggered.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type tcp
```

[Sysname-nqa-admin-test-tcp] reaction 1 checked-element probe-fail threshold-type consecutive 3 action-type trigger-only

reaction trap

Syntax **reaction trap** { **probe-failure** *consecutive-probe-failures* | **test-complete** | **test-failure** *cumulate-probe-failures* }

undo reaction trap { **probe-failure** | **test-complete** | **test-failure** }

View Any NQA test type view

Parameter **probe-failure** *consecutive-probe-failures*: Specifies to send a trap to the network management server after *consecutive-probe-failures* in an NQA test. *consecutive-probe-failures* is the number of consecutive probe failures in a test, in the range 1 to 15.

test-complete: Specifies to send a trap to indicate that the test is completed.

test-failure *cumulate-probe-failures*: Specifies to send a trap to the network management server if the total number of probe failures in an NQA test is larger than or equal to *cumulate-probe-failures*. For one test, the trap is sent only when the test is completed. *cumulate-probe-failures* is the total number of consecutive probe failures in a test, in the range 1 to 15.

Description Use the **reaction trap probe-fail** command to configure to send traps to network management server under specified conditions.

Use the **undo reaction trap probe-fail** command to restore the default.

By default, no traps are sent to the network management server.

Example # Configure to send a trap after five consecutive probe failures in an ICMP-echo test.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] reaction trap probe-failure 5
```

route-option bypass-route

Syntax **route-option bypass-route**

undo route-option bypass-route

View DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo/UDP-jitter test type view

Parameter None

Description Use the **route-option bypass-route** command to enable the routing table bypass function to test the direct connectivity to the direct destination.

Use the **undo route-option bypass-route** command to disable the routing table bypass function.

By default, the routing table bypass function is disabled.

Note that after this function is enabled, the routing table is not searched, and the packet is directly sent to the destination in a directly connected network.

Example # Enable the routing table bypass function.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] route-option bypass-route
```

source interface

Syntax **source interface** *interface-type interface-number*

undo source interface

View ICMP-echo test type view

Parameter *interface-type interface-number*: Interface type and the interface number of the source interface of a probe packet.

Description Use the **source interface** command to specify the IP address of an interface as the source IP address of ICMP-echo probe requests.

Use the **undo source interface** command to remove the IP address of an interface as the source IP address of ICMP-echo probe requests.

By default, no interface address is specified as the source IP address of ICMP test request packets.

Note that:

- If you use the **source ip** command to configure the source IP address of ICMP probe requests, the **source interface** command is invalid.
- The interface specified by the **source interface** command can only be a Layer 3 Ethernet interface or VLAN interface.
- The interface specified by the **source interface** command must be up; otherwise, the probe fails.

Related command: **source ip**.

Example # Specify the IP address of interface Ethernet 1/0 as the source IP address of ICMP-echo probe requests.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source interface ethernet 1/0
```

source ip

Syntax **source ip** *ip-address*

undo source ip

View DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo/UDP-jitter test type view

Parameter *ip-address*: Source IP address of a test operation.

Description Use the **source ip** command to configure the source IP address of ICMP probe requests in a test operation.

Use the **undo source ip** command to remove the configured source address. That is, the IP address of the interface sending a probe request serves as the source IP address of the probe request.

By default, no source IP address is specified. For an ICMP-echo test, if no source IP address is specified, but the source interface is specified, the IP address of the source interface is taken as the source IP address of ICMP probe requests.

Related command: **source interface**.

Example # Configure the source IP address of an ICMP-echo probe request as 10.1.1.1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] source ip 10.1.1.1
```

source port

Syntax **source port** *port-number*

undo source port

View SNMP/UDP-echo/UDP-jitter test type view

Parameter *port-number*: Source port number for a test operation, in the range 1 to 50000.

Description Use the **source port** command to configure the source port of ICMP probe requests in a test operation.

Use the **undo source port** command to remove the configured port number.

By default, no source port number is specified.

Example # Configure the source port number of a probe request as 8000.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type udp-echo
[Sysname-nqa-admin-test-udp-echo] source port 8000
```

tos

Syntax **tos** *value*

undo tos

View DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo/UDP-jitter test type view

Parameter *value*: Value of the ToS field in the IP header in an NQA probe packet, in the range 0 to 255.

Description Use the **tos** command to configure the value of the ToS field in the IP header in an NQA probe packet.

Use the **undo tos** command to restore the default.

By default, the ToS field in the IP header of an NQA probe packet is 0.

Example # Configure the ToS field in a IP packet header in an NQA probe packet as 1.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] tos 1
```

ttl

Syntax **ttl** *value*

undo ttl

View DLSw/FTP/HTTP/ICMP-echo/SNMP/TCP/UDP-echo/UDP-jitter test type view

Parameter *value*: Maximum number of hops a probe packet traverses in the network, in the range 1 to 255.

Description Use the **ttl** command to configure the maximum number of hops a probe packet traverses in the network.

Use the **undo ttl** command to restore the default.

By default, the maximum number of hops that a probe packet can traverse in a network is 20.

Note that after you configure the **routeopt bypass-route** command, the maximum number of hops a probe packet traverses in the network is 1.

Example # Configure the maximum number of hops that a probe request can traverse in a network as 16.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] ttl 16
```

type

Syntax **type** { **dhcp** | **dlsw** | **ftp** | **http** | **icmp-echo** | **snmp** | **tcp** | **udp-echo** | **udp-jitter** }

View NQA test group view

Parameter **dhcp**: DHCP test.

dlsw: DLSw test.

ftp: FTP test.

http: HTTP test.

icmp-echo: ICMP-echo test.

snmp: SNMP test.

tcp: TCP test.

udp-echo: UDP-echo test.

udp-jitter: UDP-jitter test.

Description Use the **type** command to configure the test type of the current test group and enter test type view.

By default, no test type is configured.

Example # Configure the test type of a test group as **FTP**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp]
```

url

Syntax **url** *url*

undo url

View HTTP test type view

Parameter *url*: Website an HTTP test visits, a string of 1 to 185 characters. It is case sensitive.

Description Use the **url** command to configure the website an HTTP test visits.

Use the **undo url** command to remove the configured website an HTTP test visits.

Note that the character string of the configured URL cannot contain spaces.

Example # Configure the website that an HTTP test visits as /index.htm.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type http
[Sysname-nqa-admin-test-http] url /index.htm
```

username (FTP test type view)

Syntax **username** *username*

undo username

View FTP test type view

Parameter *username*: Username used to log onto the FTP server, a string of 1 to 32 characters. It is case sensitive.

Description Use the **username** command to configure a username used to log onto the FTP server.

Use the **undo username** command to remove the configured username.

By default, no username is configured for logging onto the FTP server.

Related command: "password (FTP test type view)" on page 2277, "operation (FTP test type view)" on page 2276.

Example # Configure the login username as **administrator**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type ftp
[Sysname-nqa-admin-test-ftp] username administrator
```

vpn-instance (ICMP-echo test type view)

Syntax **vpn-instance** *instance*

undo vpn-instance

View ICMP-echo test type view

Parameter *instance*: VPN instance name, a string of 1 to 31 characters. It is case sensitive.

Description Use the **vpn-instance** command to specify a VPN instance.

Use the **undo vpn-instance** command to remove the specified VPN instance.

By default, no VPN instance is specified.

Example # Specify the VPN instance **vpn1**.

```
<Sysname> system-view
[Sysname] nqa entry admin test
[Sysname-nqa-admin-test] type icmp-echo
[Sysname-nqa-admin-test-icmp-echo] vpn-instance vpn1
```

150

NQA SERVER CONFIGURATION COMMANDS

You only need to configure the NQA server for UDP-jitter, TCP, and UDP-echo tests.

display nqa server status

Syntax **display nqa server status**

View Any view

Parameter None

Description Use the **display nqa server status** command to display NQA server status.

Example # Display NQA server status.

```
<Sysname> display nqa server status
nqa server is: enabled
tcp-connect:
    IP Address     Port           Status
    2.2.2.2        2000           active
udp-echo:
    IP Address     Port            Status
    3.3.3.3        3000            inactive
```

Table 602 Description on the fields of the display nqa server status command

Field	Description
tcp-connect	NQA server status in the NQA TCP test
udp-echo	NQA server status in the NQA UDP test
IP Address	IP address specified for the TCP/UDP listening service on the NQA server
Port	Port number of the TCP/UDP listening service on the NQA server

Table 602 Description on the fields of the display nqa server status command

Field	Description
Status	Listening service status: **active**: Listening service is ready; **inactive**: Listening service is not ready.

nqa server enable

Syntax **nqa server enable**

undo nqa server enable

View System view

Parameter None

Description Use the **nqa server enable** command to enable the NQA server.

Use the **undo nqa server enable** command to disable the NQA server.

By default, the NQA server is disabled.

Related command: **nqa server tcp-connect**, **nqa server udp-echo**.

Example # Enable the NQA server.

```
<Sysname> system-view
[Sysname] nqa server enable
```

nqa server tcp-connect

Syntax **nqa server tcp-connect** *ip-address port-number*

undo nqa server tcp-connect *ip-address port-number*

View System view

Parameter *ip-address*: IP address specified for the TCP listening service on the NQA server.

port-number: Port number specified for the TCP listening service on the NQA server, in the range 1 to 50000.

Description Use the **nqa-server tcp-connect** command to create a TCP listening service on the NQA server.

Use the **undo nqa-server tcp-connect** command to remove the TCP listening service created.

Note that:

- You need to configure the command on the NQA server for TCP tests only.
- The IP address and port number must be consistent with those on the NQA client and must be different from those for an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related command: **nqa server enable**.

Example # Create a TCP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server tcp-connect 169.254.10.2 9000
```

nqa server udp-echo

Syntax **nqa server udp-echo** *ip-address port-number*

undo nqa server udp-echo *ip-address port-number*

View System view

Parameter *ip-address*: IP address specified for the UDP listening service on the NQA server.

port-number: Port number specified for the UDP listening service on the NQA server, in the range 1 to 50000.

Description Use the **nqa-server udpecho** command to create a UDP listening service on the NQA server.

Use the **undo nqa-server udpecho** command to remove the UDP listening service created.

Note that:

- You need to configure the command on the NQA server for UDP-jitter and UDP-echo tests only.
- The IP address and port number must be consistent with those configured on the NQA client and must be different from those of an existing listening service.
- The IP address must be that of an interface on the NQA server. Otherwise, the configuration will be invalid.

Related command: **nqa server enable**.

Example # Create a UDP listening service by using the IP address 169.254.10.2 and port 9000.

```
<Sysname> system-view
[Sysname] nqa server udp-echo 169.254.10.2 9000
```

151 NETSTREAM CONFIGURATION COMMANDS

display ip netstream cache

Syntax **display ip netstream cache**

View Any view

Parameter None

Description Use the **display ip netstream cache** command to view configuration and status information about the NetStream cache.

Example # Display information about the NetStream cache.

```
<Sysname> display ip netstream cache
IP netstream cache information
  Stream active timeout(minute)  : 60
  Stream inactive timeout(second): 10
  Active stream entry            : 0
  Inactive stream entry          : 2000
  Stream entry been created      : 0
  Last statistics reset time     :  1/1/2000,  4:27:19
 IP packet number of different size
 1-80        81-552      553-576     577-612     613-1480    1481-1500   1501-
 0           0           0           0           0           0           0
 Protocol           Total  Packets   Stream   Packets Active(sec)   Idle(sec)
                   Streams     /Sec     /Sec   /stream     /stream     /stream
 ------------------------------------------------------------------------------
 Total                  0         0         0         0           0           0
 DstIP           DstP  SrcIP           SrcP  Pro Tos Interface        Pkts
------------------------------------------------------------------------------
 3.3.3.2         0     1.1.1.1         0     1   0     ET1/0          872
```

Table 603 Description on the fields of the display ip netstream cache command

Field	Description
Stream active timeout(minute)	Active aging timer for NetStream cache entries
Stream inactive timeout(second)	Inactive aging time for NetStream cache entries
Active stream entry	Zero or 50 active NetStream streams
IP Active stream entry	Number of active NetStream IP streams
MPLS Active stream entry	Number of active NetStream MPLS streams
IP Stream entry been statistics	Number of free NetStream IP streams that are counted
MPLS Stream entry been statistics	Number of free NetStream MPLS streams that are counted

Table 603 Description on the fields of the display ip netstream cache command

Field	Description
Inactive stream entry	Number of inactive NetStream streams
Stream entry been created	Number of NetStream cache entries that have been created
Last statistics reset time	This field is displayed only when the **reset ip netstream statistics** command; otherwise, the Last statistics reset time never field is displayed.
Last statistics reset time never	Statistics have never been cleared.
IP packet number of different size	Number of NetStream streams differentiated by packet size
1-80 81-552 553-576 577-612 613-1480 1481-1500 1501-	Packet size range, in bytes. For example, "1-80" means number of packets in size of 1 to 80 bytes, "1501-" means number of packets with size exceeding 1500 bytes
Protocol Total Streams Packets /Sec Stream /Sec Packets /stream Active(sec) /stream Idle(sec) /stream	Packet statistics differentiated by protocol type: protocol, total number of streams, number of packets per second, number of streams per second, active time for each stream, inactive time for each stream
DstIP DstP SrcIP SrcP Pro Tos Interface Pkts	Statistics of the active streams in the current NetStream cache including destination address, destination port number, source address, source port number, protocol, ToS, interface type, and number of packets

display ip netstream export

Syntax **display ip netstream export**

View Any view

Parameter None

Description Use the **display ip netstream export** command to view statistics about exported NetStream UDP packets.

Example # Display statistics about NetStream UDP packets.

```
<Sysname> display ip netstream export
 Version 5 IP export information:
  Stream source interface:     Ethernet1/0
      Stream destination IP(UDP): 10.10.0.10 (30000)
  Exported stream number:      16
  Exported UDP datagram number(failed number):      16(0)
 Version 8 AS aggregation information:
  Stream source interface:     Ethernet1/0
      Stream destination IP(UDP):  10.10.0.10 (30000)
  Exported stream number:      16
  Exported UDP datagram number(failed number):  2(0)
```

Table 604 Description on the fields of the display ip netstream export command

Field	Description
Version 5 export information	Statistics for exported version 5 statistics packets
Stream source interface	Source interface of exported UDP packets
Stream destination IP(UDP)	Destination address and port number of exported UDP packets
Exported stream number	Number of exported streams
Exported UDP datagram number(failed number)	Number of exported UDP packets (number of failed sending attempts)
Version 8 AS aggregation export information	Statistics for exported version 8 AS aggregation UDP packets. Displayed only when NetStream aggregation is enabled.
Version 8 tos-source-prefix export information	Statistics for exported version 8 ToS-source prefix aggregation packets

enable

Syntax **enable**

undo enable

View NetStream aggregation view

Parameter None

Description Use the **enable** command to enable current aggregation mode.

Use the **undo enable** command to disable current aggregation mode.

By default, no aggregation mode is enabled.

Related command: **ip netstream aggregation**.

Example # Enable NetStream AS aggregation.

```
<Sysname> system-view
[Sysname] ip netstream aggregation as
[Sysname-aggregation-as] enable
```

ip netstream

Syntax **ip netstream** { **inbound** | **outbound** }

undo ip netstream { **inbound** | **outbound** }

View Interface view

Parameter **inbound**: Enables NetStream statistics in the inbound direction of an interface.

outbound: Enables NetStream statistics in the outbound direction of an interface.

Description Use the **ip netstream** command to enable NetStream statistics in the inbound or outbound direction of the interface.

Use the **undo ip netstream** command to disable Netstream statistics in the inbound or outbound direction of the interface.

By default, NetStream statistics is disabled in both directions of the interface.

Example # Enable NetStream statistics in the inbound direction of interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ip netstream inbound
```

ip netstream aggregation

Syntax **ip netstream aggregation { as | destination-prefix | prefix | protocol-port source-prefix }**

View System view

Parameter **as**: AS aggregation by combination of source AS number, destination AS number, inbound interface index, and outbound interface index.

destination-prefix: Destination-prefix aggregation by destination AS number, destination address mask length, destination prefix, and outbound interface index.

prefix: Source and destination prefix aggregation by combination of source AS number, destination AS number, source address mask length, destination address mask length, source prefix, destination prefix, inbound interface index, and outbound interface index.

protocol-port: Protocol-port aggregation by combination of protocol number, source port, and destination port.

source-prefix: Source-prefix aggregation by combination of source AS number, source address mask length, source prefix, and inbound interface index.

Description Use the **ip netstream aggregation** command to enter NetStream aggregation view.

In NetStream aggregation view, you can enable or disable the aggregation mode, set information about source interface, destination IP address and destination port number for version 8 UDP packets.

Related command: **enable**, **ip netstream export host**, **ip netstream export source**.

Example # Enter NetStream AS aggregation view.

```
<Sysname> system-view
[Sysname] ip netstream aggregation as
[Sysname-aggregation-as]
```

ip netstream export host

Syntax **ip netstream export host** *ip-address udp-port*

undo ip netstream export host [*ip-address*]

View System view, NetStream aggregation view

Parameter *ip-address*: Destination IP address for NetStream UDP packets.

udp-port: Destination port number for NetStream UDP packets, in the range 0 to 65535.

Description Use the **ip netstream export host** command to set the destination IP address and port number for NetStream UDP packets.

Use the **undo ip netstream export host** command to restore the default.

By default, no destination IP address and port number are configured in system view and the IP address and port number in aggregation view are those configured by users in system view.

Note that:

- Different destination hosts can be configured in different aggregation views.
- You can configure up to two different destination hosts in one aggregation view. Statistics packets for a single stream are sent to all destination hosts configured in system view. Aggregation statistics packets are sent to all destination hosts configured in the aggregation view corresponding to the aggregation type.

Related command: **ip netstream aggregation**, **ip netstream export source**.

Example # Configure the destination IP address and port number for NetStream statistics packet as 172.16.105.48 and 5000 respectively.

```
<Sysname> system-view
[Sysname] ip netstream export host 172.16.105.48 5000
```

ip netstream export source

Syntax **ip netstream export source interface** *interface-type interface-number*

undo ip netstream export source

View System view, NetStream aggregation view

Parameter *interface-type interface-number*: Specifies a source interface for NetStream UDP packets by its type and number.

Description Use the **ip netstream export source interface** command to configure the source interface for NetStream UDP packets.

Use the **undo ip netstream export source** command to remove the configured source interface.

By default, the source interface is the interface from which statistics are exported.

Different source interfaces can be configured in different aggregation views.

Related command: **ip netstream aggregation**, **ip netstream** export destination.

Example # Configure the source interface for NetStream UDP packets as Ethernet 1/0.

```
<Sysname> system-view
[Sysname] ip netstream export source interface ethernet 1/0
```

ip netstream export version

Syntax **ip netstream export version** *version-number* [**origin-as** | **peer-as**]

undo ip netstream export version

View System view

Parameter *version-number*: Version number for NetStream UDP packets. Currently, version 5 is supported.

origin-as: Sets the type of AS number recorded in NetStream cache entries to origin.

peer-as: Sets the type of AS number recorded in NetStream cache entries to peer.

Description Use the **ip netstream export version** command to configure the type of AS numbers to be recorded in NetStream cache entries and the version of NetStream UDP packets.

Use the **undo ip netstream export version** command to restore the default.

By default, a single stream is sent in version 5 UDP packets and the AS option is **peer-as**.

Note that the AS numbers for the source and destination IP addresses of a stream are recorded in the statistics information. And each IP address corresponds with two AS numbers (origin and peer), the system records the AS numbers according to the AS option configured by users.

Example # Set the NetStream statistics packet version number to 5 and the AS option to **origin-as**.

```
<Sysname> system-view
[Sysname] ip netstream export version 5 origin-as
```

ip netstream max-entry

Syntax **ip netstream max-entry** *max-entries*

undo ip netstream max-entry

View System view

Parameter *max-entries*: NetStream cache size. The value ranges from 1000 to 1000000 and defaults to 10000.

Description Use the **ip netstream max-entry** command to set the NetStream cache size, meaning maximum number of entries that the NetStream cache can accommodate.

Use the **undo ip netstream max-entry** command to restore the default.

Example # Set the NetStream cache size to 5000.

```
<Sysname> system-view
[Sysname] ip netstream max-entry 5000
```

ip netstream timeout active

Syntax **ip netstream timeout active** *minutes*

undo ip netstream timeout active

View System view

Parameter *minutes*: Sets the length of the active aging timer for NetStream cache entries, in the range 1 to 60 minutes. The default value is 30 minutes.

Description Use the **ip netstream timeout active** command to set the active aging timer for NetStream cache entries.

Use the **undo ip netstream timeout active** command to restore the default.

Related command: **ip netstream timeout inactive**.

CAUTION: You can configure the active aging timer and inactive aging timer at the same time. When either one of them times out, the entry ages out. The time precision is 10 seconds.

Example # Set the active aging timer to 60 minutes.

```
<Sysname> system-view
[Sysname] ip netstream timeout active 60
```

ip netstream timeout inactive

Syntax **ip netstream timeout inactive** *seconds*

undo ip netstream timeout inactive

View System view

Parameter *seconds*: Sets the length of the inactive aging timer for NetStream cache entries, in the range 10 to 600 seconds. The default value is 30 seconds.

Description Use the **ip netstream timeout inactive** command to set the inactive aging timer for NetStream cache entries.

Use the **undo ip netstream timeout inactive** command to restore the default.

Related command: **ip netstream timeout active**.

CAUTION: You can configure the active aging timer and inactive aging timer at the same time. When either one of them times out, the entry ages out. The time precision is 10 seconds.

Example # Set the inactive aging timer to 60 seconds.

```
<Sysname> system-view
[Sysname] ip netstream timeout inactive 60
```

reset ip netstream statistics

Syntax **reset ip netstream statistics**

View User view

Parameter None

Description Use the **reset ip netstream statistics** command to age and export all stream statistics to clear the NetStream cache. The stream statistics are recounted when they age out.

Example # Age and export all stream statistics to clear the NetStream cache.

```
<Sysname> reset ip netstream statistics
```

152 NTP CONFIGURATION COMMANDS

display ntp-service sessions

Syntax **display ntp-service sessions** [**verbose**]

View Any view

Parameter **verbose**: Displays the detailed information of all NTP sessions.

Description Use the **display ntp-service sessions** command to view the information of all NTP sessions. Without the **verbose** keyword, this command will display only the brief information of all NTP service sessions.

Example # View the brief information of NTP service sessions.

```
<Sysname> display ntp-service sessions
     source       reference   stra reach   poll now  offset  delay disper
**************************************************************************
[12345]1.1.1.1    127.127.1.0  3    377    512  178   0.0    40.1   22.8
note: 1 source(master),2 source(peer),3 selected,4 candidate,5 configured
Total associations :  1
```

Table 605 Description on the fields of the display ntp-service sessions command

Field	Description
source	IP address of the clock source
reference	Reference clock ID of the clock source **1** If the reference clock is the local clock, the value of this field is related to the value of the **stra** field: ■ When the value of the **stra** field is 0 or 1, this field will be "LOCL"; ■ When the **stra** field has another value, this filed will be the IP address of the local clock. **2** If the reference clock is the clock of another device on the network, the value of this field will be the IP address of that device.
stra	Stratum level of the clock source
reach	Reachability count of the clock source. 0 indicates that the clock source in unreachable
poll	Poll interval, namely the maximum interval between successive NTP messages.

Table 605 Description on the fields of the display ntp-service sessions command

Field	Description
now	The length of time in minutes from when the last NTP message was received or when the local clock was last updated to the current time
	The time is in second by default. If the time length is greater than 2048 seconds, it is displayed in minute; if greater than 300 minutes, in hour; if greater than 96 hours, in day.
offset	The offset of the system clock relative to the reference clock, in milliseconds
delay	the roundtrip delay from the local device to the clock source, in milliseconds
disper	The maximum error of the system clock relative to the reference source.
[12345]	1: Clock source selected by the system, namely the current reference source, with a system clock stratum level of ,â§ 15
	2: Stratum level of this system source is ,â§ 15
	3: This clock source has passed the clock selection process
	4: This clock source is a candidate clock source
	5: This clock source was created by a configuration command
Total associations	Total number of associations

*When a device is working in the NTP broadcast/multicast server mode, the **display ntp-service sessions** command executed on the device will not display the NTP session information corresponding to the broadcast/multicast server, but the sessions will be counted in the total number of associations.*

display ntp-service status

Syntax **display ntp-service status**

View Any view

Parameter None

Description Use the **display ntp-service status** command to view the NTP service status information.

Example # View the NTP service status information.

```
<Sysname> display ntp-service status
Clock status: unsynchronized
 Clock stratum: 16
 Reference clock ID: none
 Nominal frequency: 100.0000 Hz
 Actual frequency: 100.0000 Hz
 Clock precision: 2^17
 Clock offset: 0.0000 ms
 Root delay: 0.00 ms
 Root dispersion: 0.00 ms
 Peer dispersion: 0.00 ms
 Reference time: 00:00:00.000 UTC Jan 1 1900(00000000.00000000)
```

Table 606 Description on the fields of the display ntp-service status command

Field	Description
Clock status	Status of the system clock
Clock stratum	Stratum level of the local clock
Reference clock ID	After the system clock is synchronized to a remote time server or a local reference source, this field indicates the address of the remote time server or the identifier of the local clock source: ■ When the local clock has a stratum level of 1, the value of this field is "LOCL"; ■ When the local clock has another value, the value of this filed is the IP address of the local clock).
Nominal frequency	The nominal frequency of the local system hardware clock
Actual frequency	The actual frequency of the local system hardware clock
Clock precision	The precision of the system clock
Clock offset	The offset of the system clock relative to the reference source
Root delay	The roundtrip delay from the local device to the primary reference source
Root dispersion	The maximum error of the system clock relative to the primary reference source.
Peer dispersion	The maximum error of the system clock relative to the reference source
Reference time	Reference timestamp

display ntp-service trace

Syntax **display ntp-service trace**

View Any view

Parameter None

Description Use the **display ntp-service trace** command view the brief information of each NTP server along the NTP server chain from the local device back to the primary reference source.

The **display ntp-service trace** command is available only if the local device can ping through all the devices on the NTP server chain; otherwise, this command will fail to display all the NTP servers on the NTP chain due to timeout.

Example # View the brief information of each NTP server from the local device back to the primary reference source.

```
<Sysname> display ntp-service trace
 server 127.0.0.1,stratum 2, offset -0.013500, synch distance 0.03154
 server 133.1.1.1,stratum 1, offset -0.506500, synch distance 0.03429
 refid LOCL
```

The information above shows an NTP server chain for the server 127.0.0.1: The server 127.0.0.1 is synchronized to the server 133.1.1.1, and the server 133.1.1.1 is synchronized to the local clock source.

Table 607 Description on the fields of the display ntp-service trace command

Field	Description
server	IP address of the NTP server
stratum	The stratum level of the corresponding system clock
offset	The clock offset relative to the upper-level clock
synch distance	The synchronization distance relative to the upper-level clock
refid	Identifier of the primary reference source. When the stratum level of the primary reference clock is 0, it is displayed as LOCL; otherwise, it is displayed as the IP address of the primary reference clock.

ntp-service access

Syntax **ntp-service access** { **peer** | **query** | **server** | **synchronization** } *acl-number*

undo ntp-service access { **peer** | **query** | **server** | **synchronization** }

View System view

Parameter **peer**: Specifies to permit full access.

query: Specifies to permit control query.

server: Specifies to permit server access and query.

synchronization: Specifies to permit server access only.

acl-number: Basic ACL number, in the range of 2000 to 2999.

Description Use the **ntp-service access** command to configure the NTP service access-control right to the local device.

Use the **undo ntp-service access** command to remove the configured NTP service access-control right to the local device.

By default, the local NTP service access-control right is set to **peer**.

From the highest NTP service access-control right to the lowest one are **peer**, **server**, **synchronization**, and **query**. When a device receives an NTP request, it will perform an access-control right match and will use the first matched right.

- *The **ntp-service access** command provides only a minimum degree of security protection. A more secure method is identity authentication.*
- *Before specifying an ACL number in the **ntp-service access** command, make sure you have already created and configured this ACL.*

Example # Configure devices on the subnet 10.10.0.0/16 to have the full access right to the local device.

```
<Sysname> system-view
[Sysname] acl number 2001
```

```
[Sysname-acl-basic-2001] rule permit source 10.10.0.0 0.0.255.255
[Sysname-acl-basic-2001] quit
[Sysname] ntp-service access peer 2001
```

ntp-service authentication enable

Syntax **ntp-service authentication enable**

undo ntp-service authentication enable

View System view

Parameter None

Description Use the **ntp-service authentication enable** command to enable NTP authentication.

Use the **undo ntp-service authentication enable** command to disable NTP authentication.

By default, NTP authentication is disabled.

Example # Enable NTP authentication.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
```

ntp-service authentication-keyid

Syntax **ntp-service authentication-keyid** *keyid* **authentication-mode md5** *value*

undo ntp-service authentication-keyid *keyid*

View System view

Parameter *keyid*: Authentication key ID, in the range of 1 to 4294967295.

authentication-mode md5 *value*: Specifies to use the MD5 algorithm for key authentication, where *value* represents authentication key and is a string of 1 to 32 characters.

Description Use the **ntp-service authentication-keyid** command to set the NTP authentication key.

Use the **undo ntp-service authentication-keyid** command to remove the set NTP authentication key.

By default, no NTP authentication key is set.

CAUTION:

- *Presently the system supports only the MD5 algorithm for key authentication.*
- *You can set a maximum of 1,024 keys for each device.*
- *If an NTP authentication key is specified as a trusted key, the key automatically changes to not trusted after you delete the key. In this case, you do not need to execute the* ***undo ntp-service reliable authentication-keyid*** *command.*

Example # Set an MD5 authentication key, with the key ID of 10 and key value of "BetterKey".

```
<Sysname> system-view
[Sysname] ntp-service authentication-keyid 10 authentication-mode md
5 BetterKey
```

ntp-service broadcast-client

Syntax **ntp-service broadcast-client**

undo ntp-service broadcast-client

View Interface view

Parameter None

Description Use the **ntp-service broadcast-client** command to configure the device to work in the NTP broadcast client mode.

Use the **undo ntp-service broadcast-client** command to remove the device as an NTP broadcast client.

Example # Configure the device to work in the broadcast client mode and receive NTP broadcast messages on Ethernet 1/1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1] ntp-service broadcast-client
```

ntp-service broadcast-server

Syntax **ntp-service broadcast-server** [**authentication-keyid** *keyid* | **version** *number*] *

undo ntp-service broadcast-server

View Interface view

Parameter **authentication-keyid** *keyid*: Specifies the key ID to be used for sending broadcast messages to broadcast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description Use the **ntp-service broadcast-server** command to configure the device to work in the NTP broadcast server mode.

Use the **undo ntp-service broadcast-server** command to remove the device as an NTP broadcast server.

Example # Configure the device to work in the broadcast server mode and send NTP broadcast messages on Ethernet 1/0, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ntp-service broadcast-server authentication-ke
yid 4 version 3
```

ntp-service in-interface disable

Syntax **ntp-service in-interface disable**

undo ntp-service in-interface disable

View Interface view

Parameters None

Description Use the **ntp-service in-interface disable** command to disable an interface from receiving NTP messages.

Use the **undo ntp-service in-interface disable** command to restore the default.

By default, all interfaces are enabled to receive NTP messages.

Examples

- On an Ethernet interface:

Disable interface Ethernet 1/0 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ntp-service in-interface disable
```

- On a VLAN interface:

Disable VLAN-interface 1 from receiving NTP messages.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ntp-service in-interface disable
```

ntp-service max-dynamic-sessions

Syntax **ntp-service max-dynamic-sessions** *number*

undo ntp-service max-dynamic-sessions

View System view

Parameter *number*: Maximum number of dynamic NTP sessions to be set up, in the range of 0 to 100.

Description Use the **ntp-service max-dynamic-sessions** command to set the maximum number of dynamic NTP sessions.

Use the **undo ntp-service max-dynamic-sessions** command to restore the maximum number of dynamic NTP sessions to the system default.

By default, the number is 100.

Example # Set the maximum number of dynamic NTP sessions to 50.

```
<Sysname> system-view
[Sysname] ntp-service max-dynamic-sessions 50
```

ntp-service multicast-client

Syntax **ntp-service multicast-client** [*ip-address*]

undo ntp-service multicast-client [*ip-address*]

View Interface view

Parameter *ip-address*: Multicast IP address, defaulting to 224.0.1.1.

Description Use the **ntp-service multicast-client** command to configure the device to work in the NTP multicast client mode.

Use the **undo ntp-service multicast-client** command to remove the device as an NTP multicast client.

Example # Configure the device to work in the multicast client mode and receive NTP multicast messages on Ethernet 1/0, and set the multicast address to 224.0.1.1.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ntp-service multicast-client 224.0.1.1
```

ntp-service multicast-server

Syntax **ntp-service multicast-server** [*ip-address*] [**authentication-keyid** *keyid* | **ttl** *ttl-number* | **version** *number*] *

undo ntp-service multicast-server [*ip-address*]

View Interface view

Parameter *ip-address*: Multicast IP address, defaulting to 224.0.1.1.

authentication-keyid *keyid*: Specifies the key ID to be used for sending multicast messages to multicast clients, where *keyid* is in the range of 1 to 4294967295. This parameter is not meaningful if authentication is not required.

ttl *ttl-number*: Specifies the TTL of NTP multicast messages, where *ttl-number* is in the range of 1 to 255 and defaults to 16.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description Use the **ntp-service multicast-server** command to configure the device to work in the NTP multicast server mode.

Use the **undo ntp-service multicast-server** command to remove the device as an NTP multicast server.

Example # Configure the device to work in the multicast server mode and send NTP multicast messages on Ethernet 1/0 to the multicast address 224.0.1.1, using key 4 for encryption, and set the NTP version to 3.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ntp-service multicast-server 224.0.1.1 version
 3 authentication-keyid 4
```

ntp-service refclock-master

Syntax **ntp-service refclock-master** [*ip-address*] [*stratum*]

undo ntp-service refclock-master [*ip-address*]

View System view

Parameter *ip-address*: IP address of the local clock, which is 127.127.1.u, where u is the NTP process ID, in the range of 0 to 3. If you do not specify *ip-address*, it defaults to 127.127.1.0.

stratum: Stratum level of the local clock, in the range of 1 to 15 and defaulting to 8.

Description Use the **ntp-service refclock-master** command to configure the local clock as a reference source for other devices.

Use the **undo ntp-service refclock-master** command to remove the local clock as a reference source.

The stratum level of a clock defines the clock precision. The value range is 1 to 16. The clock precision decreases from stratum 1 to stratum 16. A stratum 1 clock has the highest precision, and a stratum 16 clock is not synchronized and cannot be used as a reference clock.

Example # Specify the local clock as the reference source, with the stratum level of 3.

```
<Sysname> system-view
[Sysname] ntp-service refclock-master 3
```

ntp-service reliable authentication-keyid

Syntax **ntp-service reliable authentication-keyid** *keyid*

undo ntp-service reliable authentication-keyid *keyid*

View System view

Parameter *keyid*: Authentication key number, in the range of 1 to 4294967295.

Description Use the **ntp-service reliable authentication-keyid** command to specify that the created authentication key is a trusted key. When NTP authentication enabled, a client can be synchronized only to a server that can provide a trusted authentication key.

Use the **ntp-service reliable authentication-keyid** command to remove an authentication key as a trusted key.

No authentication key is configured to be trusted by default.

Example # Enable NTP authentication, specify to use MD5 encryption algorithm, with the key ID of 37 and key value of "BetterKey", and specify that this key is a trusted key.

```
<Sysname> system-view
[Sysname] ntp-service authentication enable
[Sysname] ntp-service authentication-keyid 37 authentication-mode md
5 BetterKey
[Sysname] ntp-service reliable authentication-keyid 37
```

ntp-service source-interface

Syntax **ntp-service source-interface** *interface-type interface-number*

undo ntp-service source-interface

View System view

Parameter *interface-type interface-number*: Specifies an interface by its interface type and interface number.

Description Use the **ntp-service source-interface** command to specify an interface for sending NTP messages.

Use the **undo ntp-service source-interface** command to remove the configured interface for sending NTP messages.

If you do not wish the IP address of a certain interface on the local device to become the destination address of response messages, you can use this command to specify a particular interface for sending all NTP messages, so that the source address in all NTP messages is the primary IP address of this interface.

Example # Specify that all NTP messages are to be sent out from Ethernet 1/0.

```
<Sysname> system-view
[Sysname] ntp-service source-interface ethernet 1/0
```

ntp-service unicast-peer

Syntax **ntp-service unicast-peer** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-peer [**vpn-instance** *vpn-instance-name*] { *ip-address* | *peer-name* }

View System view

Parameter **vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

ip-address: IP address of the symmetric-passive peer. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.

peer-name: Host name of the symmetric-passive peer, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the peer, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies the peer designated by *ip-address* or *peer-name* as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to its peer, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description Use the **ntp-service unicast-peer** command to designate a symmetric-passive peer for the device.

Use the **undo ntp-service unicast-peer** command to remove the symmetric-passive peer designated for the device.

No symmetric-passive peer is designated for the device by default.

- *If you specify a VPN instance name, this VPN must exist, and at least one local interface and the NTP symmetric-passive peer coexist in this VPN.*
- *If multiple VPNs have been configured on the PE and you want to synchronize the PE to a PE or CE in one of these VPNs, you need to provide* ***vpn-instance*** *vpn-instance-name in your command.*
- *If you include* ***vpn-instance*** *vpn-instance-name in the* ***undo ntp unicast-peer*** *command, the command will remove the symmetric-passive peer with the IP address of ip-address in the specified VPN; if you do not include* ***vpn-instance*** *vpn-instance-name in this command, the command will remove the symmetric-passive peer with the IP address of ip-address in the public network.*

Example # Designate the device with the IP address of 10.1.1.1 as the symmetric-passive peer of the local device, and configure the local device to run NTP version 3, and send NTP messages through Ethernet 1/0.

```
<Sysname> system-view
[Sysname] ntp-service unicast-peer 10.1.1.1 version 3 source-interfa
ce ethernet 1/0
```

ntp-service unicast-server

Syntax **ntp-service unicast-server** [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* } [**authentication-keyid** *keyid* | **priority** | **source-interface** *interface-type interface-number* | **version** *number*] *

undo ntp-service unicast-server [**vpn-instance** *vpn-instance-name*] { *ip-address* | *server-name* }

View System view

Parameter **vpn-instance** *vpn-instance-name*: Specifies a VPN instance by its name, where *vpn-instance-name* is a string of 1 to 31 characters.

ip-address: IP address of the NTP server. It must be a host address, rather than a broadcast address, a multicast address or the IP address of the local clock.

server-name: Host name of the NTP server, a string of 1 to 20 characters.

authentication-keyid *keyid*: Specifies the key ID to be used for sending NTP messages to the NTP server, where *keyid* is in the range of 1 to 4294967295.

priority: Specifies this NTP server as the first choice under the same condition.

source-interface *interface-type interface-number*: Specifies an interface for sending NTP messages. In an NTP message the local device sends to the NTP server, the source IP address is the primary IP address of this interface. *interface-type interface-number* represents the interface type and number.

version *number*: Specifies the NTP version, where *number* is in the range of 1 to 3 and defaults to 3.

Description

Use the **ntp-service unicast-server** command to designate an NTP server for the device.

Use the **undo ntp-service unicast-server** command to remove an NTP server designated for the device.

No NTP server is designated for the device by default.

- *If you specify a VPN instance name, this VPN must exist, and at least one local interface and the NTP server coexist in this VPN.*
- *If multiple VPNs have been configured on the PE and you want to synchronize the PE to a PE or CE in one of these VPNs, you need to provide* ***vpn-instance*** *vpn-instance-name in your command.*
- *If you include* ***vpn-instance*** *vpn-instance-name in the* ***undo ntp unicast-server*** *command, the command will remove the NTP server with the IP address of ip-address in the specified VPN; if you do not include* ***vpn-instance*** *vpn-instance-name in this command, the command will remove the NTP server with the IP address of ip-address in the public network.*

Example

Designate the device with the IP address of as 10.1.1.1 an NTP server for the device.

```
<Sysname> system-view
[Sysname] ntp-service unicast-server 10.1.1.1 version 3
```

153 RMON CONFIGURATION COMMANDS

display rmon alarm

Syntax **display rmon alarm** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an RMON alarm entry, in the range 1 to 65535. If no entry is specified, the configuration of all alarm entries is displayed.

Description Use the **display rmon alarm** command to display the configuration of the specified or all RMON alarm entries.

Related command: **rmon alarm**.

Example # Display the configuration of all RMON alarm table entries.

```
<Sysname> display rmon alarm
   Alarm table 1 owned by user1 is VALID.
    Samples type          : absolute
    Variable formula      : 1.3.6.1.2.1.16.1.1.1.4.1<etherStatsOctets.1>
    Sampling interval     : 10(sec)
    Rising threshold      : 50(linked with event 1)
    Falling threshold     : 5(linked with event 2)
    When startup enables  : risingOrFallingAlarm
    Latest value          : 0
```

Table 608 Description on the fields of the display rmon alarm command

Field	Description
Alarm table	Alarm entry index, 1 in this example
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples type	The sampling type (absolute in this example)
Variable formula	Formula for the sampling value
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold (When the sampling value is bigger than or equal to this threshold, a rising alarm is triggered.)
Falling threshold	Alarm falling threshold (When the sampling value is smaller than or equal to this threshold, a falling alarm is triggered.)

Table 608 Description on the fields of the display rmon alarm command

Field	Description
When startup enables	How can an alarm be triggered
Latest value	The last sampled value

display rmon event

Syntax **display rmon event** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an RMON event entry, in the range 1 to 65535. If no entry is specified, the configuration of all event entries is displayed.

Description Use the **display rmon event** command to display the configuration of the specified or all RMON event entries.

Displayed information includes event index, event owner, event description, action triggered by the event (such as sending log or trap messages), and last time the event occurred (the elapsed time since system initialization/startup) in seconds.

*If the alarm entry corresponding the configuration command is invalid (that is, the entry in the **display rmon event** command is invalid), the configuration command is not displayed in the configuration file, that is, the configuration command is not in the configuration information displayed by the **display current-configuration** command.*

Related command: **rmon event**.

Example # Display the configuration of RMON event table.

```
<Sysname> display rmon event
Event table 1 owned by user1 is VALID.
  Description: null.
  Will cause log-trap when triggered, last triggered at 0days 00h:02m:27s.
```

Table 609 Description on the fields of the display rmon event command

Field	Description
Event table	Event entry number
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Description	Description for the event
cause log-trap when triggered	The event will trigger logging and trapping.
last triggered at	Last time the event was triggered

display rmon eventlog

Syntax **display rmon eventlog** [*entry-number*]

View Any view

Parameter *entry-number*: Index of an event entry, in the range 1 to 65535. If no entry number is specified, the log information for all event entries is displayed.

Description Use the **display rmon eventlog** command to display log information for the specified or all event entries.

If you use the **rmon event** command to specify that the action of an entry includes logging, then when this event is triggered, the event log is retained in the RMON log list.

You can use the **display rmon eventlog** command to display detailed log information including event index, current event state, time the event was logged (the elapsed time in seconds since system initialization/startup), and event description.

Example # Display the RMON log information for event entry 1.

```
<Sysname> display rmon eventlog 1
Event table 1 owned by user1 is VALID.
Generates eventLog 1.1 at 0days 00h:01m:39s.
Description: The 1.3.6.1.2.1.16.1.1.1.4.1 defined in alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
Generates eventLog 1.2 at 0days 00h:02m:27s.
Description: The alarm formula defined in private alarm table 1,
less than(or =) 100 with alarm value 0. Alarm sample type is absolute.
```

Table 610 Description on the fields of the display rmon eventlog command

Field	Description
Event table	Event index
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Generates eventLog at	Time the log was created
Description	Log description

display rmon history

Syntax **display rmon history** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display rmon history** command to display RMON history control entry and last history sampling information, including bandwidth utilization, number of bad packets, and total packet number.

Related command: **rmon history**.

Example # Display RMON history entry information for interface Ethernet 1/0.

```
<Sysname> display rmon history ethernet 1/0
History control entry 1 owned by user1 is VALID
  Samples interface     : Ethernet1/0<ifEntry.642>
  Sampling interval     : 10(sec) with 10 buckets max
  Latest sampled values :
  Dropevents        :0         , octets               :0
  packets           :0         , broadcast packets    :0
  multicast packets :0         , CRC alignment errors :0
  undersize packets :0         , oversize packets     :0
  fragments         :0         , jabbers              :0
  collisions        :0         , utilization          :0
```

Table 611 Description on the fields of the display rmon history command

Field	Description
History control entry	Index of the history control entry for the interface, 1 in this example
owned by	Owner of the entry
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples Interface	The sampled interface
Sampling interval	Sampling interval
buckets max	History table size for the entry, if the specified value of the **buckets** argument exceeds the history table size supported by the device the latter is displayed.
Latest sampled values	The latest sampled values
Dropevents	Dropped packets during the sampling period
octets	The number of octets received during the sampling period
packets	The number of packets received during the sampling period
broadcastpackets	The number of broadcasts received during the sampling period
multicastpackets	The number of multicasts received during the sampling period
CRC alignment errors	The number of packets received with CRC alignment errors during the sampling period
undersize packets	The number of undersize packets received during the sampling period
oversize packets	The number of oversize packets received during the sampling period
fragments	The number of fragments received during the sampling period
jabbers	The number of jabbers received during the sampling period. (The support for the field varies with devices.)
collisions	The number of colliding packets received during the sampling period

Table 611 Description on the fields of the display rmon history command

Field	Description
utilization	Bandwidth utilization during the sampling period

display rmon prialarm

Syntax **display rmon prialarm** [*entry-number*]

View Any view

Parameter *entry-number*: Private alarm entry index, in the range 1 to 65535. If no entry is specified, the configuration of all private alarm entries is displayed.

Description Use the **display rmon prialarm** command to display the configuration of the specified or all private alarm entries.

Related command: **rmon prialarm**.

Example # Display the configuration of all private alarm entries.

```
<Sysname> display rmon prialarm
  Prialarm table 5 owned by user1 is UNDERCREATION.
    Samples type          : changeratio
    Variable formula      : ((.1.3.6.1.2.1.16.1.1.1.5.1-.1.3.6.1.2.1
.16.1.1.1.6.1)*100/.1.3.6.1.2.1.16.1.1.1.5.1)
    Description           : ifUtilization.GigabitEthernet1/0
    Sampling interval     : 10(sec)
    Rising threshold      : 892340484(linked with event 1)
    Falling threshold     : 889783312(linked with event 2)
    When startup enables  : risingOrFallingAlarm
    This entry will exist : forever
    Latest value          : 0
```

Table 612 Description on the fields of the display rmon prialarm command

Field	Description
Prialarm table	Index of the prialarm table
owned by	Owner of the entry, user1 in this example
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Samples type	Samples type
Variable formula	Variable formula
Sampling interval	Sampling interval
Rising threshold	Alarm rising threshold. An alarm event is triggered when the sampled value is greater than or equal to this threshold.
Falling threshold	Alarm falling threshold. An alarm event is triggered when the sampled value is less than or equal to this threshold.
linked with event	Event index associated with the prialarm

Table 612 Description on the fields of the display rmon prialarm command

Field	Description
When startup enables	How can an alarm be triggered
This entry will exist	The lifetime of the entry, which can be forever or span the specified period
Latest value	The last sampled value

display rmon statistics

Syntax **display rmon statistics** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display rmon statistics** command to display RMON statistics.

Related command: **rmon statistics**.

Example # Display RMON statistics for interface Ethernet 1/0.

```
<Sysname> display rmon statistics ethernet 1/0
Statistics entry 2 owned by null is VALID.
  Interface : Ethernet6/1<ifIndex.34>
  etherStatsOctets         : 0         , etherStatsPkts          : 0
  etherStatsBroadcastPkts  : 0         , etherStatsMulticastPkts : 0
  etherStatsUndersizePkts  : 0         , etherStatsOversizePkts  : 0
  etherStatsFragments      : 0         , etherStatsJabbers       : 0
  etherStatsCRCAlignErrors : 0         , etherStatsCollisions    : 0
  etherStatsDropEvents (insufficient resources): 0
  Packets received according to length:
  64     : 0         ,  65-127  : 0         ,  128-255  : 0
  256-511: 0         ,  512-1023: 0         ,  1024-1518: 0
```

Table 613 Description on the fields of the display rmon statistics command

Field	Description
Statistics entry	Statistics table entry index
VALID	Status of the entry identified by the index (VALID means the entry is valid, and UNDERCREATION means invalid. You can use the **display rmon** command to view the invalid entry and with the **display current-configuration** and **display this** commands you cannot view the corresponding **rmon** commands.)
Interface	Interface on which statistics are gathered
etherStatsOctets	The number of octets received by the interface during the statistical period
etherStatsPkts	The number of packets received by the interface during the statistical period
etherStatsBroadcastPkts	The number of broadcast packets received by the interface during the statistical period

Table 613 Description on the fields of the display rmon statistics command

Field	Description
etherStatsMulticastPkts	The number of multicast packets received by the interface during the statistical period
etherStatsUndersizePkts	The number of undersize packets received by the interface during the statistical period
etherStatsOversizePkts	The number of oversize packets received by the interface during the statistical period
etherStatsFragments	The number of undersize packets with CRC errors received by the interface during the statistical period
etherStatsJabbers	The number of oversize packets with CRC errors received by the interface during the statistical period
etherStatsCRCAlignErrors	The number of packets with CRC errors received on the interface during the statistical period
etherStatsCollisions	The number of collisions received on the interface during the statistical period
etherStatsDropEvents	Total number of drop events received on the interface during the statistical period
Packets received according to length:	Statistics of packets received according to length during the statistical period

rmon alarm

Syntax **rmon alarm** *entry-number alarm-variable sampling-interval* { **absolute** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* [**owner** *text*]

undo rmon alarm *entry-number*

View System view

Parameter *entry-number*: Alarm entry index, in the range 1 to 65535.

alarm-variable: Alarm variable, a string of 1 to 256 characters. it can be in dotted object identifier (OID) format, such as 1.3.6.1.2.1.2.1.10.1 or a node name (such as ifInOctets.1). Only variables that can be parsed into INTEGER (INTEGER, Counter, Gauge, or Time Ticks) in the ASN.1 can be used for the *alarm-variable* argument.

sampling-interval: Sampling interval, in the range 5 to 65,535 seconds.

absolute: Sets the sampling type to **absolute**.

delta: Sets the sampling type to **delta**.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2147483648 to +2147483647, and *event-entry1* represents the index of the event triggered when the rising threshold is reached. It ranges from 0 to 65535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2147483648 to +2147483647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. It ranges from 0 to 65535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon alarm** command to create an entry in the RMON alarm table.

Use the **undo rmon alarm** command to remove a specified entry from the RMON alarm table.

This command defines alarms. The generation and notification of an alarm however, is controlled by the event entry associated with it.

The following is how the system handles alarm entries:

1. Samples the alarm variables at the specified interval.
2. Compares the sampled values with the predefined threshold and does the following:
   - If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
   - If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

- *Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.*
- *When you create an entry, if the values of the specified alarm variable (alarm-variable), sampling interval (sampling-interval), sampling type (**absolute** or **delta**), rising threshold (threshold-value1) and falling threshold (threshold-value2) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 60 alarm entries.*
- *The rising alarm and falling alarm are alternate.*

Example # Add entry 1 in the alarm table and sample the node 1.3.6.1.2.1.16.1.1.1.4.1 at a sampling interval of 10 seconds in absolute sampling type. Generate event 1 when the sampled value is greater than or equal to the rising threshold of 50, and event 2 when the sampled value is lower than or equal to the falling threshold of 5. Set the owner of the entry to be user1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] rmon statistics 1
[Sysname-Ethernet1/0] quit
[Sysname] rmon alarm 1 1.3.6.1.2.1.16.1.1.1.4.1 10 absolute rising_t
hreshold 50 1 falling_threshold 5 2 owner user1
```

Remove the alarm table entry with the index of 15.

```
<Sysname> system-view
[Sysname] undo rmon alarm 15
```

rmon event

Syntax **rmon event** *entry-number* [**description** *string*] { **log** | **log-trap** *log-trapcommunity* | **none** | **trap** *trap-community* } [**owner** *text*]

undo rmon event *entry-number*

View System view

Parameter *entry-number*: Event entry index, in the range 1 to 65,535.

description *string*: Event description, a string of 1 to 127 characters.

log: Logs the event when it occurs.

log-trap *log-trapcommunity*: Log and trap events. The system records the log information and sends a trap when the event occurs. *log-trapcommunity* indicates the community name of the network management station that receives trap messages, a string of 1 to 127 characters.

none: Performs no action when the event occurs.

trap *trap-community*: Trap event. The system sends a trap with the community name being *trap-community* when the event occurs. *trap-community* represents the community name of the network management station that receives trap message, a string of 1 to 127 characters.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon event** command to create an entry in the RMON event table.

Use the **undo rmon event** command to remove a specified entry from the RMON event table.

When an event is triggered by its associated alarm in the alarm table, the event group allows you to log it, send a trap, do both, or do neither at all. This helps control the generation and notification of events.

- *When you create an entry, if the values of the specified event description (**description** string), event type (**log**, **trap**, **logtrap** or **none**), and community name (trap-community or log-trapcommunity) are identical to those of the existing event entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 60 alarm entries.*

Example # Create event 10 in the RMON event table.

```
<Sysname> system-view
[Sysname] rmon event 10 log owner user1
```

rmon history

Syntax **rmon history** *entry-number* **buckets** *number* **interval** *sampling-interval* [**owner** *text*]

undo rmon history *entry-number*

View Ethernet interface view

Parameter *entry-number:* History control entry index, in the range 1 to 65535.

buckets *number*: History table size for the entry, in the range 1 to 65,535.

interval *sampling-interval*: Sampling interval, in the range 5 to 3600 seconds.

owner *text-string*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon history** command to create an entry in the RMON history control table.

Use the **undo rmon history** command to remove a specified entry from the RMON history control table.

This command enables RMON to periodically sample and save for an interface data such as bandwidth utilization, errors, and total number of packets for later retrieval.

When you create an entry in the history table, if the specified history table size exceeds that supported by the device, the entry will be created. However, the validated value of the history table size corresponding with the entry is that supported by the device.

- *When you create an entry, if the value of the specified sampling interval (**interval** sampling-interval) is identical to that of the existing history entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 100 alarm entries.*

Related command: **display rmon history**.

Example # Create RMON history control entry 1 for interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] rmon history 1 buckets 10 interval 5 owner user1
```

Remove history control entry 15.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] undo rmon history 15
```

rmon prialarm

Syntax **rmon prialarm** *entry-number prialarm-formula prialarm-des sampling-interval* { **absolute** | **changeratio** | **delta** } **rising-threshold** *threshold-value1 event-entry1* **falling-threshold** *threshold-value2 event-entry2* **entrytype** { **forever** | **cycle** *cycle-period* } [**owner** *text*]

undo rmon prialarm *entry-number*

View System view

Parameter *entry-number*: Index of a private alarm entry, in the range 1 to 65535.

prialarm-formula: Private alarm variable formula, a string of 1 to 256 characters. The variables in the formula must be represented in OID format that starts with a point ".", the formula (.1.3.6.1.2.1.2.1.10.1)*8 for example. You may perform the basic operations of addition, subtraction, multiplication, and division on these variables. The operations should yield a long integer. To prevent errors, make sure that the result of each calculating step falls into the value range for long integers.

prialarm-des: Private alarm entry description, a string of 1 to 127 characters.

sampling-interval : Sampling interval, in the range 10 to 65,535 seconds.

absolute | **changeratio** | **delta** : Sets the sampling type to absolute, delta, or change ratio.

rising-threshold *threshold-value1 event-entry1*: Sets the rising threshold, where *threshold-value1* represents the rising threshold, in the range -2,147,483,648 to +2,147,483,647, and *event-entry 1* represents the index of the event triggered when the rising threshold is reached. It ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

falling-threshold *threshold-value2 event-entry2*: Sets the falling threshold, where *threshold-value2* represents the falling threshold, in the range -2,147,483,648 to +2,147,483,647 and *event-entry2* represents the index of the event triggered when the falling threshold is reached. It ranges from 0 to 65,535, with 0 meaning no corresponding event is triggered and no event action is taken when an alarm is triggered.

forever: Indicates that the lifetime of the private alarm entry is infinite.

cycle *cycle-period*: Sets the lifetime period of the private alarm entry, in the range 0 to 2,147,483,647 seconds.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon prialarm** command to create an entry in the private alarm table of RMON.

Use the **undo rmon prialarm** command to remove a private alarm entry from the private alarm table of RMON.

The following is how the system handles private alarm entries:

1. Samples the private alarm variables in the private alarm formula at the specified sampling interval.
2. Performs calculation on the sampled values with the formula.
3. Compares the calculation result with the predefined thresholds and does the following:
   - If the rising threshold is reached, triggers the event specified by the *event-entry1* argument.
   - If the falling threshold is reached, triggers the event specified by the *event-entry2* argument.

- *Before creating an alarm entry, define the events to be referenced in the event table with the **rmon event** command.*
- *When you create an entry, if the values of the specified alarm variable formula (prialarm-formula), sampling type (**absolute** **changeratio** or **delta**), rising threshold (threshold-value1) and falling threshold (threshold-value2) are identical to those of the existing alarm entry, the system considers their configurations the same and the creation fails.*
- *You can create up to 50 pri-alarm entries.*
- *The rising alarm and falling alarm are alternate.*

Example # Create entry 5 in the private alarm table. Calculate the private alarm variables with the (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1.16.1.1.1.5.1) formula and sample the corresponding variables at intervals of 10 seconds to get the percentage of broadcasts received on Ethernet 1/0 in the total packets. When this ratio reaches or is bigger than the rising threshold of 50, trigger event 1; when this ratio reaches or drops under the falling threshold, trigger event 2. Set the lifetime of the entry to forever and owner to user 1.

```
<Sysname> system-view
[Sysname] rmon event 1 log
[Sysname] rmon event 2 none
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] rmon statistics 1
[Sysname-Ethernet1/0] quit
[Sysname] rmon prialarm 5 (1.3.6.1.2.1.16.1.1.1.6.1*100/.1.3.6.1.2.1
.16.1.1.1.5.1)   packet Ethernet1/0 10 absolute rising_threshold 50
1 falling_threshold 5 2 entrytype forever owner user1
```

Remove private alarm entry 10.

```
<Sysname> system-view
[Sysname] undo rmon prialarm 10
```

rmon statistics

Syntax **rmon statistics** *entry-number* [**owner** *text*]

undo rmon statistics *entry-number*

View Ethernet interface view

Parameter *entry-number*: Index of statistics entry, in the range 1 to 65535.

owner *text*: Owner of the entry, a string of 1 to 127 characters. It is case sensitive and space is supported.

Description Use the **rmon statistics** command to create an entry in the RMON statistics table.

Use the **undo rmon statistics** command to remove a specified entry from the RMON statistics table.

The RMON statistics group collects information on how a monitored port is being used and records errors. Statistics include number of collisions, CRC alignment errors, number of undersize or oversize packets, number of broadcasts, number of multicasts, number of bytes received, number of packets received.

To display information for the RMON statistics table, use the **display rmon statistics** command.

- *Only one statistics entry can be created on one interface.*
- *You can create up to 100 statistics entries.*

Example # Create an entry in the RMON statistics table for interface Ethernet 1/0. The index of the entry is 20.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] rmon statistics 20 owner user1
```

154 SNMP CONFIGURATION COMMANDS

display snmp-agent local-switch fabricid

Syntax **display snmp-agent local-switch fabricid**

View Any view

Parameter **None**

Description Use the **display snmp-agent local-switch fabricid** command to display the local SNMP agent switch fabric ID.

SNMP switch fabric ID identifies an SNMP entity uniquely within an SNMP domain. SNMP switch fabric is an indispensable part of an SNMP entity. It provides the SNMP message allocation, message handling, authentication, and access control.

Example # Display the local SNMP agent switch fabric ID.

```
<Sysname> display snmp-agent local-switch fabricid
SNMP local EngineID: 800007DB7F0000013859
```

display snmp-agent community

Syntax **display snmp-agent community** [**read** | **write**]

View Any view

Parameter **read**: Displays the information of communities with read-only access right.

write: Displays the information of communities with read and write access right.

Description Use the **display snmp-agent community** command to display community information for SNMPv1 or SNMPv2c.

Example # Display the information for all the current communities.

```
<Sysname> display snmp-agent community
   Community name: aa
       Group name: aa
       Acl:2001
       Storage-type: nonVolatile
```

```
Community name: bb
    Group name: bb
    Storage-type: nonVolatile
```

Table 614 Descriptions on the fields of display snmp-agent community

Field	Description
Community name	Community name
Group name	SNMP group name
Acl	The number of the ACL in use
Storage-type	Storage type, which could be: ■ *volatile*: Information will be lost if the system is rebooted ■ *nonVolatile*: Information will not be lost if the system is rebooted ■ *permanent*: Modification permitted, but deletion forbidden ■ *readOnly*: Read only, that is, no modification, no deletion ■ *other*: Other storage types

display snmp-agent group

Syntax **display snmp-agent group** [*group-name*]

View Any view

Parameter *group-name*: Specifies the SNMP group name, a string of 1 to 32 characters, case sensitive.

Description Use the **display snmp-agent group** command to display information for the SNMP agent group, including group name, security model, MIB view, storage type, and so on. Absence of the *group-name* parameter indicates that information for all groups will be displayed.

Example # Display the information of all SNMP agent groups.

```
<Sysname> display snmp-agent group
   Group name: aa
       Security model: v3 noAuthnoPriv
       Readview: ViewDefault
       Writeview: <no specified>
       Notifyview:<no specified>
       Storage-type: nonVolatile
```

Table 615 Descriptions on the fields of the display snmp-agent group command

Field	Description
Group name	SNMP group name
Security model	Security model of the SNMP group, which can be: authPriv (authentication with privacy), authNoPriv (authentication without privacy), or noAuthNoPriv (no authentication no privacy).
Readview	The read only MIB view associated with the SNMP group
Writeview	The writable MIB view associated with the SNMP group

Table 615 Descriptions on the fields of the display snmp-agent group command

Field	Description
Notifyview	The notify MIB view associated with the SNMP group, the view with entries that can generate Trap messages
Storage-type	Storage type, which includes: volatile, nonVolatile, permanent, readOnly, and other. For detailed information, refer to Table 614.

display snmp-agent mib-view

Syntax **display snmp-agent mib-view** [**exclude** | **include** | **viewname** *view-name*]

View Any view

Parameter **exclude**: Specifies to display SNMP MIB views of the "excluded" type.

include: Specifies to display SNMP MIB views of the "included" type.

viewname *view-name*: Displays view with a specified name, where *view-name* is the name of the specified MIB view.

Description Use the **display snmp-agent mib-view** command to display SNMP MIB view information. Absence of the *view-name* parameter indicates that information for all MIB views will be displayed.

Example # Display the current SNMP MIB views.

```
<Sysname> display snmp-agent mib-view
   View name:ViewDefault
       MIB Subtree:iso
       Subtree mask:
       Storage-type: nonVolatile
       View Type:included
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpUsmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpVacmMIB
       Subtree mask:
       Storage-type: nonVolatile
       View Type:excluded
       View status:active

   View name:ViewDefault
       MIB Subtree:snmpModules.18
       Subtree mask:
       Storage-type: nonVolatile
```

```
View Type:excluded
View status:active
```

Table 616 Descriptions on the fields of the display snmp-agent mib-view command

Field	Description
View name	MIB view name
MIB Subtree	MIB subtree corresponding to the MIB view
Subtree mask	MIB subtree mask
Storage-type	Storage type
View Type	View type, which can be "included" or "excluded"
	Included indicates that all nodes of the MIB tree are included in current view.
	Excluded indicates that not all nodes of the MIB tree are included in current view.
View status	The status of MIB view

display snmp-agent statistics

Syntax **display snmp-agent statistics**

View Any view

Parameter None

Description Use the **display snmp-agent statistics** command to display SNMP statistics.

Example # Display the statistics on the current SNMP.

```
<Sysname> display snmp-agent statistics
  0 Messages delivered to the SNMP entity
  0 Messages which were for an unsupported version
  0 Messages which used an SNMP community name not known
  0 Messages which represented an illegal operation for the community supplied
  0 ASN.1 or BER errors in the process of decoding
  0 Messages passed from the SNMP entity
  0 SNMP PDUs which had badValue error-status
  0 SNMP PDUs which had genErr error-status
  0 SNMP PDUs which had noSuchName error-status
  0 SNMP PDUs which had tooBig error-status (Maximum packet size 1500)
  0 MIB objects retrieved successfully
  0 MIB objects altered successfully
  0 GetRequest-PDU accepted and processed
  0 GetNextRequest-PDU accepted and processed
  0 GetBulkRequest-PDU accepted and processed
  0 GetResponse-PDU accepted and processed
  0 SetRequest-PDU accepted and processed
  0 Trap PDUs accepted and processed
  0 Alternate Response Class PDUs dropped silently
  0 Forwarded Confirmed Class PDUs dropped silently
```

Table 617 Descriptions on the fields of the display snmp-agent statistics command

Field	Description
Messages delivered to the SNMP entity	Number of packets delivered to the SNMP agent

Table 617 Descriptions on the fields of the display snmp-agent statistics command

Field	Description
Messages which were for an unsupported version	Number of packets from a device with an SNMP version that is not supported by the current SNMP agent
Messages which used a SNMP community name not known	Number of packets that use an unknown community name
Messages which represented an illegal operation for the community supplied	Number of packets with operations that breach the access right of a community
ASN.1 or BER errors in the process of decoding	Number of packets with ASN.1 or BER errors in the process of decoding
Messages passed from the SNMP entity	Number of packets sent by an SNMP Agent
SNMP PDUs which had badValue error-status	Number of SNMP PDUs with a badValue error
SNMP PDUs which had genErr error-status	Number of SNMP PDUs with a genErr error
SNMP PDUs which had noSuchName error-status	Number of PDUs with a noSuchName error
SNMP PDUs which had tooBig error-status (Maximum packet size 1500)	Number of PDUs with a tooBig error (the maximum packet size is 1,500 bytes)
MIB objects retrieved successfully	Number of MIB objects that have been successfully retrieved
MIB objects altered successfully	Number of MIB objects that have been successfully modified
GetRequest-PDU accepted and processed	Number of get requests that have been received and processed
GetNextRequest-PDU accepted and processed	Number of getNext requests that have been received and processed
GetBulkRequest-PDU accepted and processed	Number of getBulk requests that have been received and processed
GetResponse-PDU accepted and processed	Number of get responses that have been received and processed
SetRequest-PDU accepted and processed	Number of set requests that have been received and processed
Trap PDUs accepted and processed	Number of Trap messages that have been received and processed
Alternate Response Class PDUs dropped silently	Number of dropped response packets
Forwarded Confirmed Class PDUs dropped silently	Number of forwarded packets that have been dropped

display snmp-agent sys-info

Syntax **display snmp-agent sys-info [contact | location | version] ***

View Any view

Parameter **contact**: Displays the contact information of the current network administrator.

location: Displays the location information of the current device.

version: Displays the version of the current SNMP agent.

Description Use the **display snmp-agent sys-info** command to display the current SNMP system information.

If no keyword is specified, all SNMP agent system information will be displayed.

Example # Display the current SNMP agent system information.

```
<Sysname> display snmp-agent sys-info
   The contact person for this managed node:
           Hangzhou H3C Technology Co., Ltd.

   The physical location of this node:
           Hangzhou China

   SNMP version running in the system:
           SNMPv3
```

display snmp-agent trap-list

Syntax **display snmp-agent trap-list**

View Any view

Parameter None

Description Use the **display snmp-agent trap-list** command to display the modules that can send the Trap messages and whether their Trap sending is enabled or not. If a module comprises of multiple sub-modules, then as long as one sub-module has the sending of Trap messages enabled, the whole module will be displayed as being enabled with the Trap sending.

Related command: **snmp-agent trap enable**.

Example # Display the modules that can send the Trap messages and whether their Trap sending is enabled or not.

```
<Sysname> display snmp-agent trap-list

   bgp trap enable
   configuration trap enable
   flash trap enable
   fr trap enable
   isdn trap enable
   mpls trap enable
   ospf trap enable
   standard trap enable
   system trap enable
   voice trap enable
   vrrp trap enable

   Enable traps: 11; Disable traps: 0
```

In the above output, enable indicates that the module is enabled with the Trap sending whereas disable indicates the Trap sending is disabled. By default, Trap sending is enabled on all modules that can send Trap messages. Use the **snmp-agent trap enable** command to manually configure whether the Trap sending is enabled or not.

display snmp-agent usm-user

Syntax **display snmp-agent usm-user** [**switch fabricid** *switch fabricid* | **username** *user-name* | **group** *group-name*] *

View Any view

Parameter **switch fabricid** *engineid*: Displays SNMPv3 user information for a specified switch fabric ID. *switch fabricid* indicates the SNMP switch fabric ID.

username *user-name*: Displays SNMPv3 user information for a specified user name. It is case sensitive.

group *group-name*: Displays SNMPv3 user information for a specified SNMP group name. It is case sensitive.

Description Use the **display snmp-agent usm-user** command to display SNMPv3 user information.

Example # Display SNMPv3 information for the user aa.

```
<Sysname> display snmp-agent usm-user username aa
   User name: aa
   Group name: mygroupv3
       Engine ID: 800007DB0000000000006877
       Storage-type: nonVolatile
       UserStatus: active
```

Table 618 Descriptions on the fields of the display snmp-agent usm-user command

Field	Description
User name	SNMP user name
Group name	SNMP group name
Engine ID	Engine ID for an SNMP entity
Storage-type	Storage type
UserStatus	SNMP user status

enable snmp trap updown

Syntax **enable snmp trap updown**

undo enable snmp trap updown

View Interface view

Parameter None

Description Use the **enable snmp trap updown** command to enable the sending of Trap messages for interface state change (linkup/linkdown Trap messages).

Use the **undo enable snmp trap updown** command to disable the sending of linkup/linkdown SNMP Trap messages on an interface.

By default, the sending of linkup/linkdown SNMP Trap messages is enabled.

Note that:

To enable an interface to send SNMP Trap packets when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related command: **snmp-agent target-host**, **snmp-agent trap enable**.

Example #Enable the sending of linkup/linkdown SNMP Trap messages on the port Ethernet 1/0 and use the community name public.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] enable snmp trap updown
```

snmp-agent

Syntax **snmp-agent**

undo snmp-agent

View System view

Parameter None

Description Use the **snmp-agent** command to enable SNMP agent.

Use the **undo snmp-agent** command to disable SNMP agent.

By default, SNMP agent is disabled.

Example # Disable the current SNMP agent.

```
<Sysname> system-view
[Sysname] undo snmp-agent
```

snmp-agent community

Syntax **snmp-agent community** { **read** | **write** } *community-name* [**acl** *acl-number* | **mib-view** *view-name*] *

undo snmp-agent community *community-name*

View System view

Parameter **read**: Indicates that the community has read only access right to the MIB objects, that is, the community can only inquire MIB information.

write: Indicates that the community has read and write access right to the MIB objects, that is, the community can configure MIB information.

community-name: Community name, a string of 1 to 32 characters.

view-name: MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP Agent is enabled).

acl *acl-number*: ACL for the community name, with *acl-number* indicating the ACL number, in the range 2,000 to 2,999.

mib-view *view-name*: Specifies the MIB view name associated with *community-name*, where *view-name* represents the MIB view name, a string of 1 to 32 characters. If no keyword is specified, the default view is ViewDefault (The view created by the system after SNMP agent is enabled).

Description Use the **snmp-agent community** command to configure a new SNMP community. Parameters to be configured include access right, community name, ACL, and accessible MIB views.

Use the **undo snmp-agent community** command to delete a specified community.

The community name configured with this command is only valid for the SNMP v1 and v2c agent.

Example # Configure a community with the name of comaccess that has read-only access right.

```
<Sysname> system-view
[Sysname] snmp-agent community read comaccess
```

Delete the community comaccess.

```
<Sysname> system-view
[Sysname] undo snmp-agent community comaccess
```

snmp-agent group

Syntax The following syntax applies to SNMPv1 and SNMP v2c:

snmp-agent group { **v1** | **v2c** } *group-name* [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group { **v1** | **v2c** } *group-name*

The following syntax applies to SNMPv3:

snmp-agent group v3 *group-name* [**authentication** | **privacy**] [**read-view** *read-view*] [**write-view** *write-view*] [**notify-view** *notify-view*] [**acl** *acl-number*]

undo snmp-agent group v3 *group-name* [**authentication** | **privacy**]

View System view

Parameter **v1**: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

group-name: Group name, a string of 1 to 32 characters.

authentication: Specifies the security model of the SNMP group to be authentication only (without privacy).

privacy: Specifies the security model of the SNMP group to be authentication and privacy.

read-view *read-view*: Read view, a string of 1 to 32 characters.

write-view *write-view:* Write view, a string of 1 to 32 characters.

notify-view *notify-view*: Notify view, for sending Trap messages, a string of 1 to 32 characters.

acl *acl-number*: Specifies an ACL by its number, in the range 2000 to 2999.

Description Use the **snmp-agent group** command to configure a new SNMP group and specify its access right.

Use the **undo snmp-agent group** command to delete a specified SNMP group.

By default, SNMP groups configured by the **snmp-agent group v3** command use a no-authentication-no-privacy security model.

Related command: **snmp-agent mib-view**, **snmp-agent usm-user**.

Example # Create an SNMP group group1 on an SNMPv3 enabled device, no authentication, no privacy.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 group1
```

snmp-agent local-switch fabricid

Syntax **snmp-agent local-switch fabricid** *switch fabricid*

undo snmp-agent local-switch fabricid

View System view

Parameter *switch fabricid*: Engine ID, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description Use the **snmp-agent local-switch fabricid** command to configure a local switch fabric ID for an SNMP entity.

Use the **undo snmp-agent local-switch fabricid** command to restore the default.

By default, the switch fabric ID of a device is the combination of company ID and device ID. Device ID varies by product; it could be an IP address, a MAC address, or a self-defined string of hexadecimal numbers.

Notice that if the newly configured switch fabric ID is not the same as the one used for creating the USM user, the user is invalid.

Related command: **snmp-agent usm-user**.

Example # Configure the local switch fabric ID to be 123456789A.

```
<Sysname> system-view
[Sysname] snmp-agent local-switch fabricid 123456789A
```

snmp-agent log

Syntax **snmp-agent log** { **all | get-operation | set-operation** }

undo snmp-agent log { **all** | **get-operation** | **set-operation** }

View System view

Parameter **all**: Enables logging of SNMP GET and SET operations.

get-operation: Enables logging of SNMP GET operation.

set-operation: Enables logging of SNMP SET operation.

Description Use the **snmp-agent log** command to enable SNMP logging.

Use the **undo snmp-agent log** command to restore the default.

By default, SNMP logging is disabled.

If a specified SNMP logging is enabled, when NMS performs a specified operation to SNMP Agent, the latter records the operation-related information and saves it to the information center.

Example # Enable logging of SNMP GET operation.

```
<Sysname> system-view
[Sysname] snmp-agent log get-operation
```

Enable logging of SNMP SET operation.

```
<Sysname> system-view
[Sysname] snmp-agent log set-operation
```

snmp-agent mib-view

Syntax **snmp-agent mib-view** { **excluded | included** } *view-name oid-tree* [**mask** *mask-value*]

undo snmp-agent mib-view *view-name*

View System view

Parameter **excluded**: Indicates that not all nodes of the MIB tree are included in current view.

included: Indicates that all nodes of the MIB tree are included in current view.

view-name: View name, a string of 1 to 32 characters.

oid-tree: MIB subtree. It can only be an OID string, such as 1.4.5.3.1, or an object name string, such as "system". OID is made up of a series of integers, which marks the position of the node in the MIB tree and uniquely identifies a MIB object.

mask *mask-value*: Mask for an object tree, in the range 1 to 32 hexadecimal digits. It must be an even digit.

Description Use the **snmp-agent mib-view** command to create or update MIB view information so that MIB objects can be specified.

Use the **undo snmp-agent mib-view** command to delete the current configuration.

By default, MIB view name is ViewDefault.

You can use the **display snmp-agent mib-view** command to view the access right of the default view. Also, you can use the **undo snmp-agent mib-view** command to remove the default view, after that, however, you cannot read or write all MIB nodes on Agent.

Related command: **snmp-agent group**.

Example # Create a MIB view mibtest, which includes all objects of the subtree mib2.

```
<Sysname> system-view
[Sysname] snmp-agent mib-view included mibtest 1.3.6.1
```

snmp-agent packet max-size

Syntax **snmp-agent packet max-size** *byte-count*

undo snmp-agent packet max-size

View System view

Parameter *byte-count*: Maximum number of bytes of an SNMP packet that can be received or sent by an agent, in the range 484 to 17,940. The default value is 1,500 bytes.

Description Use the **snmp-agent packet max-size** command to configure the maximum number of bytes in an SNMP packet that can be received or sent by an agent.

Use the **undo snmp-agent packet max-size** command to restore the default packet size.

Example # Configure the maximum number of bytes that can be received or sent by an SNMP agent to 1,042 bytes.

```
<Sysname> system-view
[Sysname] snmp-agent packet max-size 1042
```

snmp-agent sys-info

Syntax **snmp-agent sys-info** { **contact** *sys-contact* | **location** *sys-location* | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

undo snmp-agent sys-info { **contact** | **location** | **version** { **all** | { **v1** | **v2c** | **v3** }* } }

View System view

Parameter *sys-contact*: A string of 1 to 200 characters that describes the contact information for system maintenance.

sys-location: A string of 1 to 200 characters that describes the location of the device.

version: The SNMP version in use.

- **all**: Specifies SNMPv1, SNMPv2c, and SNMPv3.
- **v1**: SNMPv1.
- **v2c**: SNMPv2c.
- **v3**: SNMPv3.

Description Use the **snmp-agent sys-info** command to configure system information, including the contact information, the location, and the SNMP version in use.

Use the **undo snmp-agent sys-info contact** command and the **undo snmp-agent sys-info location** command to restore the default.

Use the **undo snmp-agent sys-info version** command to disable use of the SNMP function of the specified version.

By default, the location information is Hangzhou China, version is SNMPv3, and the contact is Hangzhou H3C Technology Co., Ltd.

Related command: **display snmp-agent sys-info**.

Network maintenance switch fabricers can use the system contact information to get in touch with the manufacturer in case of network failures. The system location information is a management variable under the system branch as defined in RFC1213-MIB, it identifies the location of the managed object.

Example # Configure the contact information as "Dial System Operator at beeper # 27345".

```
<Sysname> system-view
[Sysname] snmp-agent sys-info contact Dial System Operator at beeper # 27345
```

snmp-agent target-host

Syntax **snmp-agent target-host trap address udp-domain** { *ip- address* | **ipv6** *ipv6- address* } [**udp-port** *port-number*] [**vpn-instance** *vpn-instance-name*] **params securityname** *security-string* [**v1** | **v2c** | **v3** [**authentication** | **privacy**]]

undo snmp-agent target-host { *ip- address* | **ipv6** *ipv6- address* } **securityname** *security-string* [**vpn-instance** *vpn-instance-name*]

View System view

Parameter **trap**: Specifies the host to be the Trap host.

address: Specifies the IP address of the target host for the SNMP messages.

udp-domain: Indicates that the Trap message is transmitted using UDP.

ip-address: The IPv4 address of the Trap host.

ipv6 *ipv6-address:* Specifies the IPv6 address of the Trap host that receives Trap messages.

vpn-instance *vpn-instance-name*: Specifies the VPN where the host receiving Traps resides, where *vpn-instance-name* indicates the VPN instance name and is a string of 1 to 31 characters. It is case sensitive and is applicable only in a network supporting IPv4.

udp-port *port-number*: Specifies the number of the port that receives Trap messages.

params securityname *security-string*: Specifies authentication related parameters, which is SNMPv1 or SNMPv2c community name or an SNMPv3 user name, a string of 1 to 32 characters.

v1: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

authentication: Specifies the security model to be authentication without privacy.

privacy: Specifies the security model to be authentication with privacy.

Description Use the **snmp-agent target-host** command to configure the related settings for a Trap target host.

Use the **undo snmp-agent target-host** command to remove the current settings.

To enable the device to send Traps, you need to use the **snmp-agent target-host** command in combination with the **snmp-agent trap enable** and the **enable snmp trap updown** commands.

Related command: **enable snmp trap updown**, **snmp-agent trap enable**, **snmp-agent trap source**, **snmp-agent trap life**.

Example # Enable the device to send SNMP Traps to 10.1.1.1, using the community name of "public".

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
```

Enable the device to send SNMP Traps to the device which is in VPN 1 and has an IP address of 10.1.1.1, using the community name of **public**.

```
<Sysname> system-view
[Sysname] snmp-agent trap enable standard
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 vp
n-instance vpn1 params securityname public
```

snmp-agent trap enable

Syntax **snmp-agent trap enable** [**bgp** | **configuration** | **flash** | **fr** | **isdn** | **mpls** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **voice** | **vrrp** [**authfailure** | **newmaster**]]

undo snmp-agent trap enable [**bgp** | **configuration** | **flash** | **fr** | **mpls** | **ospf** [*process-id*] [*ospf-trap-list*] | **standard** [**authentication** | **coldstart** | **linkdown** | **linkup** | **warmstart**]* | **system** | **voice** | **vrrp** [**authfailure** | **newmaster**]]

View System view

Parameter **bgp**: Enables the sending of BGP Trap packets.

configuration: Enables the sending of configuration Trap packets.

flash: Enables the sending of FLASH Trap packets.

fr: Enables the sending of Trap packets in the event of Frame Relay virtual link change.

isdn: Enables the sending of ISDN Trap packets.

mpls: Enables the sending of LSP Trap packets.

ospf [*process-id*] [*ospf-trap-list*]: Enables the sending of OSPF Trap packets. The parameter *process-id* is the process ID and *spf-trap-list* is the Trap packet list.

standard: Enables the sending of standard Trap packets.

- **authentication**: Enables the sending of authentication failure Trap packets in the event of authentication failure.
- **coldstart**: Sends coldstart Trap packets when the device restarts.
- **linkdown**: Sends linkdown Trap packets when the port is in a linkdown status. It should be configured globally.
- **linkup**: Sends linkup Trap packets when the port is in a linkup status. It should be configured globally.

warmstart: Sends warmstart Trap packets when the SNMP restarts.

system: Sends H3C-SYS-MAN-MIB (a private MIB) Trap packets.

voice: Enables the sending of voice Trap packets.

vrrp [**authfailure | newmaster**]: Sends VRRP Trap packets.

- **authfailure**: Sends authentication failure VRRP Trap packets.
- **newmaster**: Enables the sending of VRRP newmaster Trap packets when the device becomes the Master.

Description Use the **snmp-agent trap enable** command to enable the device to send Trap messages globally.

Use the **undo snmp-agent trap enable** command to disable the device from sending Trap messages.

By default, the device is enabled to send all types of Trap messages.

Note that:

To enable an interface to send SNMP Trap packets when its state changes, you need to enable the Link up/down Trap packet transmission function on an interface and globally. Use the **enable snmp trap updown** command to enable this function on an interface, and use the **snmp-agent trap enable** [**standard** [**linkdown** | **linkup**] *] command to enable this function globally.

Related command: **snmp-agent target-host**, **enable snmp trap updown**.

Example # Enable the device to send SNMP authentication failure packets to 10.1.1.1, using the community name of "public".

```
<Sysname> system-view
[Sysname] snmp-agent target-host trap address udp-domain 10.1.1.1 pa
rams securityname public
[Sysname] snmp-agent trap enable standard authentication
```

snmp-agent trap if-mib link extended

Syntax **snmp-agent trap if-mib link extended**

undo snmp-agent trap if-mib link extended

View System view

Parameter None

Description Use the **snmp-agent trap if-mib link extended** command to extend the standard linkUp/linkDown Trap messages defined in RFC. The extended linkUp/linkDown Trap messages comprise the standard linkUp/linkDown Trap messages defined in RFC plus interface description and interface type.

Use the **undo snmp-agent trap if-mib link extended** command to restore the default.

By default, standard linkUp/linkDown Trap messages defined in RFC are used.

Note that after this command is configured, the device sends extended linkUp/linkDown Trap messages. If the extended messages are not supported on NMS, the device may not be able to resolute the messages.

Example # Extend standard linkUp/linkDown Trap messages defined in RFC.

```
<Sysname> system-view
[Sysname] snmp-agent trap if-mib link extended
```

snmp-agent trap life

Syntax **snmp-agent trap life** *seconds*

undo snmp-agent trap life

View System view

Parameter *seconds*: Time-out time, in the range 1 to 2,592,000 seconds.

Description Use the **snmp-agent trap life** command to configure the life time for Traps, which will be discarded when their life time expires.

Use the **undo snmp-agent trap life** command to restore the default life time for Trap packets.

By default, the life time for SNMP Traps is 120 seconds.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**.

Example # Configure the life time for Trap packets as 60 seconds.

```
<Sysname> system-view
[Sysname] snmp-agent trap life 60
```

snmp-agent trap queue-size

Syntax **snmp-agent trap queue-size** *size*

undo snmp-agent trap queue-size

View System view

Parameter *size*: The queue size for the Trap messages, in the range 1 to 1,000.

Description Use the **snmp-agent trap queue-size** command to configure the size of the Trap queue.

Use the **undo snmp-agent trap queue-size** command to restore the default queue size.

By default, up to 100 Trap messages can be stored in the Trap queue.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**, **snmp-agent trap life**.

Example # Configure the size of the Trap queue to 200.

```
<Sysname> system-view
[Sysname] snmp-agent trap queue-size 200
```

snmp-agent trap source

Syntax **snmp-agent trap source** *interface-type* { *interface-number* | *interface-number.subnumber* }

undo snmp-agent trap source

View System view

Parameter *interface-type* { *interface-number* | *interface-number.subnumber* }: Specifies the interface type and interface number. The parameter *interface-number* represents the main interface number. The parameter *subnumber* represents the subinterface number and ranges from 1 to 4,094.

Description Use the **snmp-agent trap source** command to specify the source IP address contained in the Trap message.

Use the **undo snmp-agent trap source** command to restore the default.

By default, SNMP chooses the IP address of an interface to be the source IP address of the Trap message.

Use this command to trace a specific event by the source IP address of a Trap message.

Before you can configure the IP address of a particular interface as the source IP address of the Trap message, ensure that the interface already exists and that it has a legal IP address. Otherwise, it is likely that the configurations will either fail or be invalid.

Related command: **snmp-agent trap enable**, **snmp-agent target-host**.

Example # Configure the IP address for the port Ethernet 1/0 to be the source address for Trap packets.

```
<Sysname> system-view
[Sysname] snmp-agent trap source ethernet 1/0
```

snmp-agent usm-user

Syntax The following syntax applies to SNMPv1 and SNMPv2c:

snmp-agent usm-user { **v1** | **v2c** } *user-name group-name* [**acl** *acl-number*]

undo snmp-agent usm-user { **v1** | **v2c** } *user-name group-name*

The following syntax applies to SNMPv3:

snmp-agent usm-user v3 *user-name group-name* [**authentication-mode** { **md5** | **sha** } *auth-password* [**privacy-mode** { **aes128** | **des56** } *priv-password*]] [**acl** *acl-number*]

undo snmp-agent usm-user v3 *user-name group-name* { **local** | **switch fabricid** *switch fabricid-string* }

View System view

Parameter **v1**: SNMPv1.

v2c: SNMPv2c.

v3: SNMPv3.

user-name: User name, a string of 1 to 32 characters. It is case sensitive.

group-name: Group name, a string of 1 to 32 characters. It is case sensitive.

acl *acl-number*: Specifies a basic ACL, in the range 2,000 to 2,999.

authentication-mode: Specifies that the security mode is authentication.

- **md5**: Specifies the authentication protocol to be HMAC-MD5-96.
- **sha**: Specifies the authentication protocol to be HMAC-SHA-96.

auth-password: Authentication password, a string of 1 to 64 characters.

privacy: Specifies that the security mode is privacy.

- **aes128**: Specifies the privacy protocol to be advanced encryption standard (AES).
- **des56**: Specifies the privacy protocol to be data encryption standard (DES).

priv-password: The privacy password, a string of 1 to 64 characters.

local: Specifies to use a local switch fabric ID.

switch fabricid *switch fabricid*-string: Specifies the switch fabric ID string, an even number of hexadecimal characters, in the range 10 to 64. Its length must not be an odd number, and the all-zero and all-F strings are invalid.

Description Use the **snmp-agent usm-user** command to add a user to an SNMP group.

Use the **undo snmp-agent usm-user** command to delete a user from an SNMP group.

Note that the validity of a user depends on the switch fabric ID of the SNMP agent. If the switch fabric ID used for creating the user is not identical to the current switch fabric ID, the user is invalid.

For SNMPv1 and SNMPv2c, this command means adding of a new SNMP group. For SNMPv3, this command adds a new user to an SNMP group.

Related command: **snmp-agent group**, **snmp-agent community**, **snmp-agent local-switch fabricid**.

Example # Add a user John to the SNMP group Johngroup. Configure the security model to be authentication, the authentication protocol to be HMAC-MD5-96, and the authentication password to be hello.

```
<Sysname> system-view
[Sysname] snmp-agent group v3 Johngroup
[Sysname] snmp-agent usm-user v3 John Johngroup authentication-mode md5 hello
```

155 FILE SYSTEM CONFIGURATION COMMANDS

- *A file name cannot be longer than 64 characters (including drive letter and a string terminator. If the drive letter is "CF: /", the file name can be at most [64-1-4] = 59 characters in length; or, errors will occur in file operation. Typically, the file name is recommended to be not more than 16 characters.*
- *A file name cannot contain ASCII characters (ASCII>=128) or invisible characters (ASCII<33).*
- *A filename cannot contain characters such as """, "'", "?", "", "Space", "*", "|", "<"">"/", ":", ">" or "~".*
- *." can be included in a filename, but it cannot be the first or the last character of the filename and there cannot be two consecutive "."s.*

cd

Syntax **cd** *directory*

View User view

Parameter *directory*: Name of the target directory.

Description Use the **cd** command to change the current directory.

Example # Change the current directory to cf:.

```
<Sysname> cd cf:
```

Return to the upper directory.

```
<Sysname> cd ..
```

Return to the root directory.

```
<Sysname> cd /
```

copy

Syntax **copy** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file.

fileurl-dest: Name of the target file.

Description Use the **copy** command to copy a file.

Example # Copy file testcfg.cfg and save it as tt.cfg.

```
<Sysname> copy testcfg.cfg tt.cfg
Copy cf:/config.cfg to cf:/tt.cfg?[Y/N]:y

%Copy file cf:/testcfg.cfg to cf:/tt.cfg...Done.
```

delete

Syntax **delete** [**/unreserved**] *file-url*

View User view

Parameter **/unreserved**: Permanently deletes the specified file, and the deleted file can never be restored.

file-url: Name of the file to be deleted. Asterisks (*) are acceptable as wildcards. For example, to remove files with the expansion of txt, you may use the **delete *.txt** command

Description Use the **delete** command to remove a specified file from the storage device to the recycle bin, where you can restore the file with the **undelete** command or permanently delete it with the **reset recycle-bin** command.

The **dir /all** command displays the files removed to the recycle bin. These files are enclosed in pairs of brackets.

This command supports the wildcard *.

CAUTION: *If you delete two files in different directories but with the same filename, only the last one is retained in the recycle bin.*

Example # Remove the file tt.cfg from the root directory.

```
<Sysname> delete tt.cfg
Delete cf:/tt.cfg?[Y/N]:y
.
%Delete file cf:/tt.cfg...Done.
```

dir

Syntax **dir** [/**all** | *file-url*]

View User view

Parameter **/all**: Displays all files (including those in the recycle bin).

file-url: Name of the file or directory to be displayed. Asterisks (*) are acceptable as wildcards. For example, to display files with the .txt extension under the current directory, you may use the **dir ***.txt command.

Description Use the **dir** command to display information about all visible files and folders in the current directory.

Use the **dir /all** command to display information about all files and folders on your device, including hidden files, hidden subfiles and those in the recycle bin. The names of these deleted files are enclosed in pairs of brackets ([ ]).

The **dir** *file-url* command displays information about a file or folder.

This command supports the wildcard *.

Example # Display information about all files and folders.

```
Directory of cf:/
   0   drw-          -  Jul 18 2006 10:32:44   logfile
   1   -rw-  16044820  Oct 30 2006 15:46:58   main.bin
   2   -rwh          4  Oct 31 2006 14:08:16   snmpboots
   3   -rw-       2012  Oct 30 2006 16:17:28   config.cfg
   4   -rwh        828  Oct 30 2006 16:17:26   private-data.txt
   5   drw-          -  Oct 31 2006 14:28:24   test
   6   -rw-  16044820  Oct 31 2006 14:34:24   [mytest.bin]
252344 KB total (220800 KB free)
File system type of cf: FAT16
[ ] indicates this file is in the recycle bin.
```

execute

Syntax **execute** *filename*

View System view

Parameter *filename*: Name of a batch file with a .bat extension.

Description Use the **execute** command to execute the specified batch file.

Batch files are command line files. Executing a batch file is to execute a set of command lines in the file.

You should not include invisible characters in a batch file. If an invisible character is found during the execution, the batch process will abort and the commands that have been executed cannot be cancelled.

Not every command in a batch file is sure to be executed. For example, if a certain command is not correctly configured, the system omits this command and goes to the next one.

A batch file does not support hot backup.

Each configuration command in a batch file must be a standard configuration command, meaning the valid configuration information which can be displayed with the **display current-configuration** command after this command is configured successfully; otherwise, this command may not be executed correctly.

Example # Execute the batch file test.bat in the root directory.

```
<Sysname> system-view
[Sysname] execute test.bat
```

file prompt

Syntax **file prompt** {**alert** | **quiet** }

View System view

Parameter **alert**: Enables the system to warn you about operations that may bring undesirable results such as file corruption or data loss.

quiet: Disables the system to warn you about any operation.

Description Use the **file prompt** command to set a prompt mode for file operations.

By default, the prompt mode is **alert**.

Note that when the prompt mode is set to **quiet**, the system does not warn for any file operation. To prevent undesirable consequents resulted from misoperations, the **alert** mode is preferred.

Example # Set the file operation prompt mode to **alert**.

```
<Sysname> system-view
[Sysname] file prompt alert
```

fixdisk

Syntax **fixdisk** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **fixdisk** command to restore the space of a storage device when it becomes unavailable because of some abnormal operation.

Example # Restore the space of the CF card.

```
<Sysname> fixdisk cf:
%Fixdisk cf: completed.
```

format

Syntax **format** *device*

View User view

Parameter *device*: Storage device name.

Description Use the **format** command to format a storage device.

CAUTION: *Formatting a device results in loss of all the files and these files cannot be restored. In particular, if there is startup configuration file on a CF card, formatting the storage device results in loss of the startup configuration file.*

Example # Format the CF card.

```
<Sysname> format cf:
All data on cf: will be lost, proceed with format? [Y/N]:y
./
%Format cf: completed.
```

mkdir

Syntax **mkdir** *directory*

View User view

Parameter *directory*: Name of a directory.

Description Use the **mkdir** command to create a subdirectory under the specified directory on the storage device.

The name of the subdirectory to be created must be unique under the specified directory.

This command does not allow you to create multiple directory levels at one time. For instance, to create a subdirectory "cf:/test/mytest", the test directory must have been created.

Example # Create a directory named test.

```
<Sysname> mkdir test
% Created dir cf:/test
```

create a subdirectory named mytest under test.

```
<Sysname>mkdir test/mytest
%Created dir cf:/test/mytest
```

more

Syntax **more** *file-url*

View User view

Parameter *file-url*: File name.

Description Use the **more** command to display the contents of the specified file.

So far, this command is valid only for .txt files.

Example # Display the contents of file test.txt.

```
<Sysname> more test.txt
AppWizard has created this test application for you.
This file contains a summary of what you will find in each of the fi
les that make up your test application.
Test.dsp
This file (the project file) contains information at the project lev
el and is used to build a single project or subproject. Other users
can share the project (.dsp) file, but they should export the makefi
les locally.
```

Display the content of the file testcfg.cfg.

```
<Sysname> more testcfg.cfg

#
 version 5.20, Beta 1201, Standard
#
 sysname Sysname
#
 configure-user count 5
#
vlan 2
#
return
<Sysname>
```

mount

Syntax **mount** *device*

View User view

Parameter *device*: Name of a storage device.

Description Use the **mount** command to mount a hot swappable storage device, such as a CF card, a USB device, etc (excluding Flash). This command is effective only when the device is in unmounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the board when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the **mount** command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device.

Related command: **umount**.

- *The support of this command varies with devices.*
- *For a device supporting partitioning, this command can only **mount** a partition device rather than the storage device.*

Example # Mount a CF card on a centralized device.

```
<Sysname> mount cf:
% Mount cf: successfully.
%Apr 23 01:50:00:628 2003 System VFS/0/LOG:
cf: mounted into slot 0.
```

On a device supporting partitioning, mount the third partition device on the CF card.

```
<Sysname> mount cf2:
% Mount cf2: successfully.
%Apr 23 01:50:00:628 2003 Sysname VFS/5/LOG:
cf2: mounted into slot 4.
```

move

Syntax **move** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file.

fileurl-dest: Name of the target file.

Description Use the **move** command to move a file.

Example # Move the file cf:/test/sample.txt to cf:/sample.txt.

```
<Sysname> move cf:/test/sample.txt cf:/sample.txt
Move cf:/test/sample.txt to cf:/sample.txt ?[Y/N]:y
% Moved file cf:/test/sample.txt to cf:/sample.txt
```

pwd

Syntax **pwd**

View User view

Parameter None

Description Use the **pwd** command to display the current path.

If the current path is not set, the operation will fail.

Example # Display the current path.

```
<Sysname> pwd
cf:
```

rename

Syntax **rename** *fileurl-source fileurl-dest*

View User view

Parameter *fileurl-source*: Name of the source file or directory.

fileurl-dest: Name of the target file or directory.

Description Use the **rename** command to rename a file or directory.

The target file name must be unique under the current path.

Example # Rename the file sample.txt as sample.bak.

```
<Sysname> rename sample.txt sample.bak
Rename cf:/sample.txt to cf:/sample.bak?[Y/N]:y

% Renamed file cf:/sample.txt to cf:/sample.bak
```

reset recycle-bin

Syntax **reset recycle-bin** [**/force**]

View User view

Parameter **/force**: Empties the recycle bin.

Description Use the **reset recycle-bin** command to permanently remove deleted file or files from the recycle bin.

Unlike this command, the **delete** *file-url* command only moves files to the recycle bin.

Example # Empty the recycle bin.

```
<Sysname> reset recycle-bin
Clear cf:/tt.cfg ?[Y/N]:y
Clearing files from cf may take a long time. Please wait...
.
%Cleared file cf:/~/tt.cfg.
```

rmdir

Syntax **rmdir** *directory*

View User view

Parameter *directory*: Name of the directory.

Description Use the **rmdir** command to remove a directory.

The directory must be an empty one. If it is not, first delete all files and subdirectory under it with the **delete** command.

Example # Remove directory mydir.

```
<Sysname> rmdir mydir
Rmdir cf:/mydir?[Y/N]:y

%Removed directory cf:/mydir.
```

umount

Syntax **umount** *device*

View User view

Parameter *device*: Storage device name (for example flash or cf) on a device that does not support storage device partitioning; partition device name (for example cf0 or cf1) on a device supporting storage device partitioning.

Description Use the **umount** command to unmount a hot swappable storage device, such as a CF card or a USB device, excluding Flash. This command is effective only when the device is in mounted state.

By default, a storage device is in the mounted state, that is, you can use it without mounting it.

Note that:

- Do not remove the storage device or swap the board when mounting or unmounting the device, or when you are processing files on the storage device. Otherwise, the file system could be damaged.
- When a storage device is connected to a low version system, the system may not be able to recognize the device automatically, you need to use the mount command for the storage device to function normally.
- Before removing a mounted storage device from the system, you should first unmount it to avoid damaging the device. By default, a storage device is in the mounted state. You can use it without mounting it.

Related command: **mount**.

Example # Unmount a CF card on a device.

```
<Sysname> umount cf:
% Umount cf: successfully.
%Apr 23 01:49:20:929 2003 System VFS/5/LOG:
cf: umounted from slot 0.
```

undelete

Syntax **undelete** *file-url*

View User view

Parameter *file-url*: Name of the file to be restored.

Description Use the **undelete** command to restore a file from the recycle bin.

If another file with the same name exists under the same path, the undelete operation will cause it to be overwritten and the system will ask you whether to continue.

Example # Restore file sample.bak from the recycle bin.

```
<Sysname> undelete sample.bak
Undelete cf:/sample.bak ?[Y/N]:y
% Undeleted file cf:/sample.bak
```

156 CONFIGURATION FILE MANAGEMENT COMMANDS

backup startup-configuration

Syntax **backup startup-configuration to** *dest-addr* [*dest-filename*]

View User view

Parameter *dest-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

dest-filename: Target filename used to save the next startup configuration file on the server.

Description Use the **backup startup-configuration** command to backup the startup configuration file (for next startup) using a filename you specify. If you do not specify this filename, the original filename will be used.

- With a device that supports main/backup function, this command only backups the main configuration file for next startup.
- With a device that does not support main/backup function, this command backups the configuration file for next startup.

Presently, the device uses TFTP to implement backup operation.

Example # Backup the configuration file for next startup on the TFTP server with IP address 2.2..2.2, using the filename config.cfg.

```
<Sysname> backup startup-configuration to 2.2.2.2 config.cfg
Backup next startup-configuration file to 2.2.2.2, please wait...
finished!
<Sysname>
```

display saved-configuration

Syntax **display saved-configuration** [**by-linenum**]

View Any view

Parameter **by-linenum**: Identifies each line of displayed information with a line number.

Description Use the **display saved-configuration** command to display the initial configuration file saved in the storage device.

In case the device malfunctions after being powered on, if you find some configurations are not validated or incorrect, you may use this command to identify the problem.

If you do not use the configuration file when the device starts up, meaning the displayed startup configuration file is NULL after you execute the **display startup** command, no information is displayed when you execute the **display saved-configuration** command; if you have saved the configuration file after the device starts up, the information last saved in the configuration file is displayed.

Related command: **save**, **reset saved-configuration**, and **display current-configuration** on page 2412.

Example # Display the configuration file saved in the storage device.

```
<Sysname> display saved-configuration
#
 Version 5.20, Beta 1105
#
 sysname Mydevice
#
 local-user abc password simple abc
#
 tcp window 8
#
interface Aux1/0
 link-protocol ppp
#
interface Ethernet1/1
#
interface Ethernet1/2
#
interface Ethernet1/3
 ip address 10.110.101.17 255.255.255.0
#
interface NULL0
#
ospf 1
#
 ip route-static 10.12.0.0 255.255.0.0 Ethernet 1/0
#
user-interface con 0
user-interface aux 0
user-interface vty 0 4
 authentication-mode none
#
return
```

The configurations are displayed in the order of global, port, and user interface.

display startup

Syntax **display startup**

View Any view

Parameter None

Description Use the **display startup** command to display the configuration file used at this startup and the one used for next startup.

Related command: **startup saved-configuration**.

Example # Display the configuration file used at this startup and the one used for next startup (main/backup attribute not supported).

```
<Sysname> display startup
  Current startup saved-configuration file:          cf:/testcfg.cfg
  Next startup saved-configuration file:             cf:/testcfg.cfg
```

Display the configuration file used at this startup and the one used for next startup (main/backup attribute supported).

```
<Sysname> display startup
  Current startup saved-configuration file:          cf:/config.cfg
  Next main startup saved-configuration file:        cf:/config.cfg
  Next backup startup saved-configuration file:      NULL
```

reset saved-configuration

Syntax **reset saved-configuration** [**backup** | **main**]

View User view

Parameter **backup**: Erases the backup configuration file.

main: Erases the main configuration file.

Description Use the **reset saved-configuration** command to erase the configuration file saved in the storage device.

Note that:

- The **reset saved-configuration** [**main**] command erases the configuration file which has the main attribute only; while for the configuration file which has both the main and backup attributes, the command erases its main attribute.
- The **reset saved-configuration backup** command erases the configuration file which has the backup attribute only; while for the configuration file which

has both the main and backup attributes, the command erases its backup attribute.

CAUTION: *This command will permanently delete the configuration file on the device. Use it with caution.*

Related command: **save**, **display saved-configuration**.

Example # Erase the configuration file saved in the storage device. (main/backup attribute not supported)

```
<Sysname> reset saved-configuration
The saved configuration will be erased.
Are you sure? [Y/N]:y
Configuration in the device is being cleared.
Please wait .......
Configuration in the device is cleared.
```

Erase the configuration file saved in the storage device. (main/backup attribute supported)

```
<Sysname> reset saved-configuration backup
The saved configuration will be erased.
Are you sure? [Y/N]:y
Configuration in the device is being cleared.
Please wait .......
Configuration in the device is cleared.
```

restore startup-configuration

Syntax **restore startup-configuration from** *src-addr src-filename*

View User view

Parameter *src-addr*: IP address or name of a TFTP server. The address cannot be an IPv6 address.

src-filename: Filename of the configuration file to be downloaded from the specified server.

Description Use the **restore startup-configuration** command to download the configuration file from the specified TFTP server for the next startup of the device.

- This command will download the configuration without copying it to the backup board.
- If a device supports main/backup configuration file, the file downloaded is the main configuration file.
- If a device does not support main/backup configuration file, the command downloads the configuration file for next startup.

If the file to be downloaded has the same filename as an existing file on the main or backup board, you will be prompted whether you want to overwrite the

existing file or not. In addition, both the main board and the backup board are assumed to use the storage device of the same type when checking filename or downloading the configuration file (both to the root directory of the main board or backup board); otherwise, the restoration fails.

Example # Download the configuration file config.cfg for the next startup from the TFTP server whose IP address is .2.2.2.2.

```
<Sysname> restore startup-configuration from 2.2.2.2 config.cfg
Restore next startup-configuration file from 2.2.2.2. Please wait...finished!
Now restore next startup-configuration file from main to slave board, Please w
ait...finished!
```

save

Syntax **save** [*file-name* | [**safely**] [**backup** | **main**]]

View Any view

Parameter *file-name*: File name, whose suffix must be .cfg.

safely: Sets the configuration saving mode to safe. If this argument is not specified, the configuration file is saved in fast mode.

backup: Saves the configuration as the backup configuration file.

main: Saves the configuration as the main configuration file.

Description Use the **save** command to save the current configuration to the specified configuration file. If no filename is specified, the system saves the configuration file in an interactive way. In this way, you can use the default path (the configuration file for next startup) or enter a filename to specify a new path, but the suffix of the filename must be ".cfg" and the path must be the path of the storage device on the active main board (AMB).

For a device that supports main/backup configuration file:

- The command saves the current configuration to the main configuration file if the **main** or **backup** keyword is not specified.
- If you specified a filename, but the filename does not exist, the system will create this file and save the configuration into this file. The file attribute is neither main nor backup.
- If you specified a filename and this file exists, the system will save the configuration into this file. The file attribute is the original attribute of the file.

Note that:

- The **reset saved-configuration** [**main**] command erases the configuration file which has the main attribute only; while for the configuration file which has both the main and backup attributes, the command erases its main attribute.

- The **reset saved-configuration backup** command erases the configuration file which has the backup attribute only; while for the configuration file which has both the main and backup attributes, the command erases its backup attribute.

Related command: **reset saved-configuration**, **display current-configuration** on page 2412, **display saved-configuration**.

Example # Save the current configuration file to the default directory (main/backup attribute not supported)

```
<Sysname> save
The current configuration will be written to the device.
Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cf:/testcfg.cfg]
(To leave the existing filename unchanged, press the enter key):
cf:/testcfg.cfg exists, overwrite?[Y/N]:y

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration cf:/testcfg.cfg. Please wait...
.
Configuration is saved to cf successfully.
<Sysname>
```

Save the current configuration to the backup configuration file (main/backup attribute supported)

```
<Sysname> save backup
The current configuration will be written to the device.
Are you sure? [Y/N]:y
Please input the file name(*.cfg)[cf:/text.cfg]
(To leave the existing filename unchanged, press the enter key):bb.cfg

Validating file. Please wait...
Now saving current configuration to the device.
Saving configuration cf:/bb.cfg. Please wait...
....
Configuration is saved to cf successfully.
<Sysname>
```

startup saved-configuration

Syntax **startup saved-configuration** *cfgfile* [**backup** | **main**]

undo startup saved-configuration

View User view

Parameter *cfgfile*: Configuration file name.

backup: Sets the configuration file as backup configuration file.

main: Sets the configuration file as main configuration file.

Description Use the **startup saved-configuration** command to specify a configuration file for next startup.

Use the **undo startup saved-configuration** command to start up with an empty configuration, which means startup with the initial configuration of the system. If the configuration file has main/backup attribute, this command erases the attribute but does not delete the file.

The specified file must be ended with a .cfg extension and saved in the root directory of the storage device. (For a device supporting storage device partitioning, the file must be saved on the first partition).

When the configuration file supports main/backup attribute:

- For a normal configuration file, after the execution of the **startup saved-configuration** *cfgfile* **main** command, the configuration file becomes a main configuration file.
- For a normal configuration file, after the execution of the **startup saved-configuration** *cfgfile* **backup** command, the configuration file becomes a backup configuration file.
- For a main configuration file, after the execution of the **startup saved-configuration** *cfgfile* **backup** command, the configuration file has both main and backup attributes.
- For a backup configuration file, after the execution of the **startup saved-configuration** *cfgfile* **main** command, the configuration file has both main and backup attributes.
- If main/backup attribute is not specified, the file is set as a main configuration file.
- If a main configuration file already exists when you set a new file as the main configuration file, the main attribute of the existing file will be erased to allow only one main configuration file in the system.
- If a backup configuration file already exists when you set a new file as the backup configuration file, the backup attribute of the existing file will be erased to allow only one backup configuration file in the system.

Related command: **display startup**.

Example # Specify a configuration file for next startup (main/backup attribute not supported).

```
<Sysname> startup saved-configuration testcfg.cfg
Please wait ....... Done!
```

Specify a backup configuration file for next startup (main/backup attribute supported).

```
<Sysname> startup saved-configuration testcfg.cfg backup
Please wait......Done!
```

157
FTP SERVER CONFIGURATION COMMANDS

display ftp-server

Syntax **display ftp-server**

View Any view

Parameter None

Description Use the **display ftp-server** command to display the FTP server configuration of the device.

After configuring FTP parameters, you may verify them with this command.

Related command: **ftp timeout** and **ftp update**.

Example # Display the FTP server configuration.

```
<Sysname> display ftp-server
   FTP server is running
   Max user number:              1
   User count                     1
   Timeout value(in minute):     30
   Put Method:                   fast
```

The output indicates that the FTP server is running with support to only one concurrent login user; now one logged-in user is present; timeout of the user is 30 minutes, and FTP update mode is fast.

display ftp-user

Syntax **display ftp-user**

View Any view

Parameter None

Description Use the **display ftp-user** command to display the detailed information of current FTP users.

Example # Display the detailed information of FTP users.

```
<Sysname> display ftp-user
UserName             HostIP    Port    Idle              HomeDir
     aaaa             5.5.5.6     1027        0                   cf:
```

Table 619 Description on the fields of the display ftp-user command

Field	Description
UserName	Name of the present logged-in user
HostIP	IP address of the present logged-in user
Port	Port which the present logged-in user is using
Idle	Duration time of the current FTP connection
HomeDir	Specified path of the present logged-in user

free ftp user

Syntax **free ftp user** *username*

View User view

Parameter *username:* Username used when the FTP connection to be released is established.

Description Use the **free ftp user** command to manually release the FTP connection established with the specified username.

Note that if the user to be released is transmitting a file, the connection between the user and the FTP server is terminated after the file transmission.

Example # Manually release the FTP connection established with username of ftpuser.

```
<Sysname> free ftp user ftpuser
Are you sure to free FTP user ftpuser? [Y/N]:y
<Sysname>
```

ftp server enable

Syntax **ftp server enable**

undo ftp server

View System view

Parameter None

Description Use the **ftp server enable** command to enable the FTP server.

Use the **undo ftp server** command to disable the FTP server.

By default, the FTP server is disabled to prevent attacks.

Example # Disable the FTP server.

```
<Sysname> system-view
[Sysname] undo ftp server
% Close FTP server
```

ftp timeout

Syntax **ftp timeout** *minute*

undo ftp timeout

View System view

Parameter *minute*: Idle-timeout timer in minutes, in the range 1 to 35791. The default is 30 minutes.

Description Use the **ftp timeout** command to set the idle-timeout timer.

Use the **undo ftp timeout** command to restore the default.

After you log onto the FTP server, you set up an FTP connection. When the connection is disrupted, the FTP server, if not notified, cannot realize that and maintains the connection all the same. To address this problem, you can set an idle-timeout timer to have the FTP server disconnected if no information is received or/and transmitted before the timer expires.

Example # Set the idle-timeout timer to 36 minutes.

```
<Sysname> system-view
[Sysname] ftp timeout 36
```

ftp update

Syntax **ftp update** { **fast** | **normal** }

undo ftp update

View System view

Parameter *fast*: Fast update.

normal: Normal update.

Description Use the **ftp update** command to set the file update mode that the FTP server uses while receiving data.

Use the **undo ftp update** command to restore the default, namely, the normal mode.

Example # Set the FTP update mode to normal.

```
<Sysname> system-view
[Sysname] ftp update normal
```

158
FTP CLIENT CONFIGURATION COMMANDS

- *You must use the **ftp** command to enter FTP client view for configurations under this view. For details, refer to "ftp" on page 2378.*
- *The prompt information in the examples of this section varies with devices.*

ascii

Syntax **ascii**

View FTP client view

Parameter None

Description Use the **ascii** command to set the file transfer mode to ASCII for the FTP connection.

FTP provides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the file transfer mode is ASCII.

Example # Set the file transfer mode to ASCII.

```
[ftp] ascii
200 Type set to A.
```

binary

Syntax **binary**

View FTP client view

Parameter None

Description Use the **binary** command to set the file transfer mode to binary (also called flow mode).

FTP usprovides two file transfer modes: ASCII and binary. To transfer text files, use the ASCII mode; to transfer program files, use the binary mode.

By default, the transfer mode is ASCII mode.

Example # Set the file transfer mode to binary.

```
[ftp] binary
200 Type set to I.
```

bye

Syntax **bye**

View FTP client view

Parameter None

Description Use the **bye** command to disconnect from the remote FTP server and exit to user view.

Example # Terminate the connection with the remote FTP server and exit to user view.

```
[ftp] bye
221 Server closing.
```

cd

Syntax **cd** *pathname*

View FTP client view

Parameter *pathname*: Path name.

Description Use the **cd** command to change the current working directory on the remote FTP server.

You can use this command to access another authorized directory on the FTP server.

Example # Change the current working directory to cf:/logfile.

```
[ftp] cd cf:/logfile
250 CWD command successful.
```

cdup

Syntax **cdup**

View FTP client view

Parameter None

Description Use the **cdup** command to exit the current directory and enter the upper directory of the FTP server.

Example # Change the current working directory path to the upper directory.

```
[ftp] cdup
200 CDUP command successful.
```

close

Syntax **close**

View FTP client view

Parameter None

Description Use the **close** command to terminate the connection to the FTP server, but remain in FTP client view.

This command is equal to the **disconnect** command.

Example # Terminate the connection to the FTP server and remain in FTP client view.

```
[ftp] close
221 Server closing.
[ftp]
```

debugging

Syntax **debugging**

undo debugging

View FTP client view

Parameters None

Description Use the **debugging** command to enable FTP client debugging.

Use the **undo debugging** command to disable FTP client debugging.

By default, FTP client debugging is disabled.

Examples # The device serves as the FTP client. Enable FTP client debugging and use the active mode to download file **sample.file** from the current directory of the FTP server.

```
<Sysname> terminal monitor
<Sysname> terminal debugging
<Sysname> ftp 192.168.1.46
Trying 192.168.1.46 ...
Press CTRL+K to abort
Connected to 192.168.1.46.
220 FTP service ready.
User(192.168.1.46:(none)):ftp
331 Password required for ftp.
Password:
230 User logged in.

[ftp]undo passive
[ftp] debugging
[ftp] get sample.file

---> PORT 192,168,1,44,4,21
200 Port command okay.
 The parsed reply is 200
---> RETR sample.file
150 Opening ASCII mode data connection for sample.file.
 The parsed reply is 150
FTPC: File transfer started with the signal light turned on.
FTPC: File transfer completed with the signal light turned off.
.226 Transfer complete.
FTP: 3304 byte(s) received in 4.889 second(s), 675.00 byte(s)/sec.

[ftp]
```

Table 620 Description on the fields of the debugging command

Field	Description
---> PORT	Give an FTP order, with data port numbers being...
The parsed reply is	The received reply code, which is defined in RFC 959.
---> RETR	Download the file
FTPC: File transfer started with the signal light turned on.	File transfer starts, and the signal light is turned on.
FTPC: File transfer completed with the signal light turned off.	File transfer is completed, and the signal light is turned off.

delete

Syntax **delete** *remotefile*

View FTP client view

Parameter *remotefile*: File name.

Description Use the **delete** command to delete a specified file on the remote FTP server.

To do this, you must be a user with the delete permission on the FTP server.

Example # Delete file temp.c.

```
[ftp] delete temp.c
250 DELE command successful.
```

dir

Syntax **dir** [*remotefile* [*localfile*]]

View FTP client view

Parameter *remotefile*: Name of the file or directory on the remote FTP server.

localfile: Name of the local file to save the displayed information.

Description Use the **dir** command to view detailed information of the files and subdirectories under the current directory on the remote FTP server.

Use the **dir** *remotefile* command to display the detailed information of the specified file or directory on the remote FTP server.

Use the **dir** *remotefile localfile* command to display the detailed information of the specified file or directory on the remote FTP server, and save the displayed information into a local file specified by the *localfile.*argument.

*The **ls** command can only display the names of files and directories, whereas the **dir** command can display other related information of the files and directories, such as the size, the date they were created.*

Example # View the information of the file ar-router.cfg, and save the result to aa.txt.

```
[ftp] dir ar-router.cfg aa.txt
227 Entering Passive Mode (192,168,1,50,17,158).
125 ASCII mode data connection already open, transfer starting for a
r-router.cfg.
....226 Transfer complete.
FTP: 67 byte(s) received in 4.600 second(s), 14.00 byte(s)/sec.
```

View the content of aa.txt

```
[ftp] quit
<Sysname> more aa.txt
-rwxrwxrwx   1 noone    nogroup      3077 Jun 20 15:34 ar-router.cfg
```

disconnect

Syntax **disconnect**

View FTP client view

Parameter None

Description Use the **disconnect** command to disconnect from the remote FTP server but remain in FTP client view.

This command is equal to the **close** command.

Example # Disconnect from the remote FTP server but remain in FTP client view.

```
[ftp] disconnect
221 Server closing.
```

display ftp client configuration

Syntax **display ftp client configuration**

View Any view

Parameter None

Description Use the **display ftp client configuration** command to display the configuration information of the FTP client.

Currently this command displays the configuration information of the source address. If the currently valid source address is the source IP address, this command displays the configured source IP address; if it is the source interface, this command displays the configured source interface.

Related command: **ftp client source**.

Example # Display the current configuration information of the FTP client.

```
<Sysname> display ftp client configuration
The source IP address is 192.168.0.123
```

ftp

Syntax **ftp** [*server-address* [*service-port*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]]

View User view

Parameter *server-address*: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range of 0 to 65535. The default value is 21.

interface *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on this interface is the source address of the transmitted packets. If no primary IP address is configured on the source interface, the connection fails.

ip *source-ip-address:* The source IP address of the current FTP client. This source address must be the one that has been configured on the device.

Description Use the **ftp** command to log onto the remote FTP server and enter FTP client view.

Note that:

- This command applies to IPv4 network.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.
- The priority of the source address specified with this command is higher than that with the **ftp client source** command. If you specify the source address with the **ftp client source** command first and then with the **ftp** command, the source address specified with the **ftp** command is used to communicate with the FTP server.

Related command: **ftp client source**.

Example # Log from the current device Sysname1 onto the device Sysname2 with the IP address of 192.168.0.211. The source IP address of the packets sent is 192.168.0.212.

```
<Sysname1> ftp 192.168.0.211 source ip 192.168.0.212
Trying 192.168.0.211 ...
Press CTRL+K to abort
Connected to 192.168.0.211.
220 FTP Server ready
User(192.168.0.211:(none)):abc
331 Password required for abc
Password:
230 Login OK
[ftp]
```

ftp client source

Syntax **ftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo ftp client source

View System view

Parameter **interface** *interface-type interface-number*: Source interface for the FTP connection, including interface type and interface number. The primary IP address configured on the source interface is the source IP address of the packets sent by

FTP. If no primary IP address is configured on the source interface, the connection fails.

ip *source-ip-address:* Source IP address of the FTP connection. It must be an IP address configured on the device.

Description Use the **ftp client source** command to configure the source address of the transmitted FTP packets from the FTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with an FTP server.

Note that:

- The source address includes the source interface and the source IP address. If you use the **ftp client source** command to specify the source interface and the source IP address, the newly specified source IP address overwrites the original one and vice versa.
- If the source address is specified with the **ftp client source** command and then with the **ftp** command, the source address specified with the latter one is used to communicate with the FTP server.
- The source address specified with the **ftp client source** command is valid for all **ftp** connections and the source address specified with the **ftp** command is valid only for the current **ftp** connection.

Related command: **display ftp client configuration**.

Example # Specify the source IP address of the FTP client as 2.2.2.2.

```
<Sysname> system-view
[Sysname] ftp client source ip 2.2.2.2
```

Specify the source interface of the FTP client as Ethernet1/0.

```
<Sysname> system-view
[Sysname] ftp client source interface ethernet 1/0
```

ftp ipv6

Syntax **ftp ipv6** [*server-address* [*service-port*] [**source ipv6** *source-ipv6-address*] [**-i** *interface-type interface-number*]]

View User view

Parameter *server-address*: IP address or host name of the remote FTP server.

service-port: Port number of the FTP server, in the range 0 to 65535. The default value is 21.

source ipv6 *source-ipv6-address*: Specifies a source IPv6 address for transmitted FTP packets. This address must be an IPv6 address that has been configured on the device.

-i *interface-type interface-number*: Specifies the type and number of the egress interface. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 829).

Description Use the **ftp ipv6** command to log onto the FTP server and enter FTP client view.

Note that:

- This command applies to IPv6 network.
- If you use this command without specifying any parameters, you will simply enter the FTP client view without logging onto the FTP server.
- If you specify the parameter, you will be asked to enter the username and password for accessing the FTP server.

Example # Log onto the FTP server with IPv6 address 3000::200

```
<Sysname> ftp ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
[ftp]
```

get

Syntax **get** *remotefile* [*localfile*]

View FTP client view

Parameter *remotefile*: File name on the remote FTP server.

localfile: Local file name.

Description Use the **get** command to download a file from a remote FTP server and save it.

If no name is specified, the local file uses the name of the source file on the FTP server by default.

Example # Download file testcfg.cfg and save it as aa.cfg.

```
[ftp]get testcfg.cfg aa.cfg
```

```
227 Entering Passive Mode (192,168,1,50,17,163).
125 ASCII mode data connection already open, transfer starting for testcfg.cfg.
.....226 Transfer complete.
FTP: 5190 byte(s) received in 7.754 second(s), 669.00 byte(s)/sec.
```

lcd

Syntax **lcd**

View FTP client view

Parameter None

Description Use the **lcd** command to display the local directory of the FTP client.

Example # Display the local directory.

```
[ftp] lcd
FTP: Local directory now cf:/temp
```

ls

Syntax **ls** [*remotefile*] [*localfile*]]

View FTP client view

Parameter *remotefile*: Filename or directory on the remote FTP server.

localfile: Name of a local file used to save the displayed information.

Description Use the **ls** command to view the information of all the files and subdirectories under the current directory of the remote FTP server. The file names and subdirectory names are displayed.

Use the **ls** *remotefile* command to view the information of a specified file or subdirectory.

Use the **ls** *remotefile localfile* command view the information of a specified file or subdirectory, and save the result to a local file specified by the *localfile* argument.

The ls command can only display the names of files and directories, whereas the dir command can display other related information of the files and directories, such as the size, the date they are created.

Example # View the information of all files and subdirectories under the current directory of the FTP server.

```
[ftp] ls
227 Entering Passive Mode (192,168,1,50,17,165).
125 ASCII mode data connection already open, transfer starting for *.
ar-router.cfg
```

```
logfile
mainar.bin
arbasicbtm.bin
ftp
test
bb.cfg
testcfg.cfg
226 Transfer complete.
FTP: 87 byte(s) received in 0.132 second(s) 659.00 byte(s)/sec.
```

View the information of directory logfile, and save the result to file aa.txt.

```
[ftp] ls logfile aa.txt
227 Entering Passive Mode (192,168,1,50,17,166).
125 ASCII mode data connection already open, transfer starting for logfile.
.....226 Transfer complete.
FTP: 9 byte(s) received in 0.094 second(s) 95.00 byte(s)/sec.
```

View the content of file aa.txt

```
[ftp] quit
<Sysname> more aa.txt
logfile
```

mkdir

Syntax **mkdir** *directory*

View FTP client view

Parameter *directory*: Directory name.

Description Use the **mkdir** command to create a subdirectory under the specified directory on the remote FTP server.

To do this, you must be a user with the permission on the FTP server.

Example # Create subdirectory mytest on the current directory of the remote FTP server.

```
[ftp] mkdir mytest
257 " cf:/mytest" new directory created.
```

open

Syntax **open** *server-address* [*service-port*]

View FTP client view

Parameter *server-address*: IP address or host name of a remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535, with the default value of 21.

Description Use the **open** command to log onto the IPv4 FTP server under FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

Related command: **close**

Example # In FTP client view, log onto the FTP server with the IP address of 192.168.1.50..

```
<Sysname> ftp
[ftp] open 192.168.1.50
Trying 192.168.1.50 ...
Press CTRL+K to abort
Connected to 192.168.1.50.
220 FTP service ready.
User(192.168.1.50:(none)):aa
331 Password required for aa.
Password:
230 User logged in.

[ftp]
```

open ipv6

Syntax **open ipv6** *server-address* [*service-port*] [**-i** *interface-type interface-number*]

View FTP client view

Parameter *server-address*: IP address or host name of the remote FTP server.

service-port: Port number of the remote FTP server, in the range 0 to 65535. The default value is 21.

-i *interface-type interface-number*: Specifies the egress interface by it type and number. This parameter can be used only in case that the FTP server address is the link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 829).

Description Use the **open ipv6** command to log onto IPv6 FTP server in FTP client view.

At login, you will be asked to enter the username and password for accessing the FTP server. If your input is correct, the login succeeds; otherwise, it fails.

Related command: **close**

Example # Log onto the FTP server (with IPv6 address 3000::200) in FTP client view.

```
<Sysname> ftp
[ftp] open ipv6 3000::200
Trying 3000::200 ...
Press CTRL+K to abort
```

```
Connected to 3000::200.
220 Welcome!
User(3000::200:(none)): MY_NAME
331 Please specify the password.
Password:
230 Login successful.
```

passive

Syntax **passive**

undo passive

View FTP client view

Parameter None

Description Use the **passive** command to set the data transmission mode to passive.

Use the **undo passive** command to set the data transmission mode to active.

The default transmission mode is passive.

Example # Set the data transmission mode to passive.

```
[ftp] passive
FTP: passive is on
```

put

Syntax **put** *localfile* [*remotefile*]

View FTP client view

Parameter *localfile*: Local file name.

remotefile: Name of the file to be saved on the remote FTP server.

Description Use the **put** command to upload a file to the remote FTP server.

If no name is assigned to the file to be saved on the FTP server, the name of the source file is used by default.

Example # Upload source file cc.txt to the remote FTP server and save it as dd.txt.

```
[ftp] put cc.txt dd.txt
227 Entering Passive Mode (192,168,1,50,17,169).
125 ASCII mode data connection already open, transfer starting for dd.txt.
226 Transfer complete.
FTP: 9 byte(s) sent in 0.112 second(s), 80.00byte(s)/sec.
```

pwd

Syntax **pwd**

View FTP client view

Parameter None

Description Use the **pwd** command to display the working directory on the remote FTP server.

Example # Display the working directory on the remote FTP server.

```
[ftp] pwd
257 "cf:/temp" is current directory.
```

quit

Syntax **quit**

View FTP client view

Parameter None

Description Use the **quit** command to disconnect from the remote FTP server and exit to user view.

Example # Disconnect from the remote FTP server and exit to user view.

```
[ftp] quit
221 Server closing.
<Sysname>
```

remotehelp

Syntax **remotehelp** [*protocol-command*]

View FTP client view

Parameter *protocol-command*: FTP command.

Description Use the **remotehelp** command to display the help information of FTP-related commands supported by the remote FTP server.

If no parameter is specified, FTP-related commands supported by the remote FTP server are displayed.

Example # Display FTP commands supported by the remote FTP server.

```
[ftp] remotehelp
214-Here is a list of available ftp commands
    Those with '*' are not yet implemented.
   USER    PASS    ACCT*  CWD    CDUP   SMNT*  QUIT   REIN*
   PORT    PASV    TYPE   STRU*  MODE*  RETR   STOR   STOU*
   APPE*   ALLO*   REST*  RNFR*  RNTO*  ABOR*  DELE   RMD
   MKD     PWD     LIST   NLST   SITE*  SYST   STAT*  HELP
   NOOP*   XCUP    XCWD   XMKD   XPWD   XRMD
214 Direct comments to H3C company.
```

Display the help information for the **user** command.

```
[ftp] remotehelp user
214 Syntax: USER <sp> <username>.

[ftp]
```

Table 621 Description on the fields of the remotehelp command

Field	Description
214-Here is a list of available ftp commands	The following is an available FTP command list.
Those with '*' are not yet implemented.	Those commands with "*" are not yet implemented.
USER	Username
PASS	Password
CWD	Change the current working directory
CDUP	Change to parent directory
SMNT*	File structure setting
QUIT	Quit
REIN*	Re-initialization
PORT	Port number
PASV	Passive mode
TYPE	Request type
STRU*	File structure
MODE*	Transmission mode
RETR	Download a file
STOR	Upload a file
STOU*	Store unique
APPE*	Appended file
ALLO*	Allocation space
REST*	Restart
RNFR*	Rename the source
RNTO*	Rename the destination
ABOR*	Abort the transmission
DELE	Delete a file
RMD	Delete a folder
MKD	Create a folder
PWD	Print working directory
LIST	List files

Table 621 Description on the fields of the remotehelp command

Field	Description
NLST	List file description
SITE*	Orient a parameter
SYST	Display system parameters
STAT*	State
HELP	Help
NOOP*	No operation
XCUP	Extension command, the same meaning as CUP
XCWD	Extension command, the same meaning as CWD
XMKD	Extension command, the same meaning as MKD
XPWD	Extension command, the same meaning as PWD
XRMD	Extension command, the same meaning as RMD
Syntax: USER <sp> <username>.	Syntax of the **user** command: user (keyword) + space + *username*

rmdir

Syntax **rmdir** *directory*

View FTP client view

Parameter *directory*: Directory name on the remote FTP server.

Description Use the **rmdir** command to remove a specified directory from the FTP server.

Note that only authorized users are allowed to use this command.

Note that:

- The directory to be deleted must be empty, meaning you should delete all files and the subdirectory under the directory before you delete a directory. For the deletion of files, refer to "delete" on page 2352.
- After you execute the **rmdir** command, the files in the remote recycle bin under the directory will be automatically deleted.

Example # Delete the cf:/temp1 directory from the FTP server.

```
[ftp] rmdir cf:/temp1
200 RMD command successful.
```

user

Syntax **user** *username* [*password*]

View FTP client view

Parameter *username*: Other login username.

password: Login password.

Description Use the **user** command to relog onto the currently accessing FTP server with other username after you have logged onto the FTP server.

Before using this command, you must configure the corresponding username and password on the FTP server; otherwise, you login fails and the FTP connection is closed.

Example # User ftp1 has logged onto the FTP server and relogs onto the current FTP server with the username of ftp2. (Suppose username ftp2 and password 123123123123 have been configured on the FTP server).

```
[ftp] user ftp2
331 Password required for ftp2.
Password:
230 User logged in.

[ftp]
```

verbose

Syntax **verbose**

undo verbose

View FTP client view

Parameter None

Description Use the **verbose** command to enable the verbose function to display detailed prompt information.

Use the **undo verbose** command to disable the verbose function.

By default, the verbose function is enabled.

Example # Enable the verbose function.

```
[ftp] verbose
FTP: verbose is on
```

159 TFTP CLIENT CONFIGURATION COMMANDS

display tftp client configuration

Syntax **display tftp client configuration**

View Any view

Parameter None

Description Use the **display tftp client configuration** command to display the configuration information of the TFTP client.

Related command: **tftp client source**.

Example # Display the current configuration information of the TFTP client.

```
<Sysname> display tftp client configuration
The source IP address is 192.168.0.123
```

Currently this command displays the source address configuration information. If the currently valid source address is the source IP address, the configured source IP address is displayed; if the currently valid address is the source interface, the configured source interface is displayed.

tftp-server acl

Syntax **tftp-server** [**ipv6**] **acl** *acl-number*

undo tftp-server [**ipv6**] **acl**

View System view

Parameter **ipv6**: References an IPv6 ACL. If it is not specified, an IPv4 ACL is referenced.

acl-number: Number of basic ACL, in the range 2000 to 2999.

Description Use the **tftp-server acl** command to reference an ACL to control access to the TFTP server. Users can use the configured rules in ACL to allow or prevent the use of TFTP server in a network.

Use the **undo tftp-server acl** command to remove the access restriction.

For more information about ACL, refer to *"IPv4 ACL Configuration Commands" on page 2087 and "IPv6 ACL Configuration Commands" on page 2103.*

Example # Reference ACL 2000 to control access to the TFTP application in IPv4.

```
<Sysname> system-view
[Sysname] acl number 2000
[Sysname-acl-basic-2000] rule permit source 1.1.1.1 0
[Sysname-acl-basic-2000] quit
[Sysname] tftp-server acl 2000
```

Associate IPv6 ACL 2001 with TFTP application in Ipv6.

```
<Sysname> system-view
[Sysname] acl ipv6 number 2001
[Sysname-acl6-basic-2001] rule permit source 2030:5060::9050/64
[Sysname-acl6-basic-2001] quit
[Sysname] tftp-server ipv6 acl 2001
```

tftp

Syntax **tftp** *server-address* { **get** | **put** | **sget** } *source-filename* [*destination-filename*] [**source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }]

View User view

Parameter *server-address:* IP address or host name of a TFTP server.

source-filename: Source file name.

destination-filename: Destination file name.

get: Downloads a file in normal mode.

put: Uploads a file.

sget: Downloads a file in secure mode.

source: Configures parameters for source address binding.

- **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.
- **ip** *source-ip-address:* Specifies a source IP address for transmitted TFTP packets. This source address must be the one that has been configured on the device.

Description Use the **tftp** command to upload files from the local device to a TFTP server or download files from the TFTP server to the local device.

- If no destination file name is specified, the saved file uses the source file name.
- The priority of the source address specified with this command is higher than that with the **tftp client source** command. If you use the **tftp client source** command to specify the source address first and then with the **tftp** command, the latter one is adopted.

This command applies to IPv4 network.

Related command: **tftp client source**.

Example # Download the config.cfg file from the TFTP server with the IP address of 192.168.0.98 and save it as config.bak. Specify the source IP address to be 192.168.0.92.

```
<Sysname> tftp 192.168.0.98 get config.cfg config.bak source ip 192.168.0.92
  .
  File will be transferred in binary mode
  Downloading file from remote tftp server, please wait...<HardReturn
  TFTP:     2143 bytes received in 0 second(s)
  File downloaded successfully.
```

Upload the config.cfg file from the storage device to the default path of the TFTP server with the IP address of 192.168.0.98 and save it as config.bak. Specify the source IP interface to be Ethernet 1/0.

```
<Sysname> tftp 192.168.0.98 put config.cfg config.bak source interface Ether
net 1/0
.
  File will be transferred in binary mode
  Sending file to remote tftp server. Please wait... <HardReturn
  TFTP:     2143 bytes sent in 0 second(s).
  File uploaded successfully.
```

tftp client source

Syntax **tftp client source** { **interface** *interface-type interface-number* | **ip** *source-ip-address* }

undo tftp client source

View System view

Parameter **interface** *interface-type interface-number*: Specifies the source interface by its type and number. The primary IP address configured on the source interface is the source IP address of the packets sent by FTP. If no primary IP address is configured on the source interface, the transmission fails.

ip *source-ip-address:* The source IP address of the TFTP connection. It must be an IP address configured on the device.

Description Use the **tftp client source** command to configure the source address of the TFTP packets from the TFTP client.

Use the **undo telnet client source** command to restore the default.

By default, a device uses the IP address of the interface determined by the routing protocol as the source IP address to communicate with a TFTP server.

Note that:

- The source address includes the source interface and the source IP, if you use the **tftp client source** command to specify the source interface and the source IP, the newly specified source IP overwrites the original one and vice versa.
- If the source address is specified with the **tftp client source** command and then with the **tftp** command, use the latter one.
- The source address specified with the **tftp client source** command is valid for all **tftp** connections and the source address specified with the **tftp** command is valid for the current **tftp** command.

Related command: **display tftp client configuration**.

Example # Specify the source IP address of the TFTP client to 2.2.2.2.

```
<Sysname> system-view
[Sysname] tftp client source ip 2.2.2.2
```

Specify the source interface of the TFTP client to be Ethernet 1/0.

```
<Sysname> system-view
[Sysname] ftp client source interface ethernet 1/0
```

tftp ipv6

Syntax **tftp ipv6** *tftp-ipv6-server* [**-i** *interface-type interface-number*] { **get** | **put** } *source-file* [*destination-file*]

View User view

Parameter *tftp-ipv6-server*: IPv6 address or host name (a string of 1 to 46 characters) of a TFTP server.

-i *interface-type interface-number*: Specifies the egress interface by its type and number. This parameter can be used only in case that the TFTP server address is a link local address and the specified egress interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 829).

get: Downloads a file.

put: Uploads a file.

source-filename: Source filename.

destination-filename: Destination filename. If not specified, this filename is the same as the source filename.

Description Use the **tftp ipv6** command to download a specified file from a TFTP server or upload a specified local file to a TFTP server.

This command applies to IPv6 network.

Example # Download filetoget.txt from TFTP server.

```
<Sysname> tftp ipv6 fe80::250:daff:fe91:e058 -i ethernet 1/0 get fil
etoget. txt

File will be transferred in binary mode
  Downloading file from remote tftp server, please wait...
  TFTP:       32 bytes received in 5 second(s).
  File downloaded successfully
```

160 SYSTEM MAINTAINING COMMANDS

ping

Syntax **ping** [**ip**] [**-a** *source-ip* | **-c** *count* | **-f** | **-h** *ttl* | **-i** *interface-type interface-number* | **-m** *interval* | **-n** | **-p** *pad* | **-q** | **-r** | **-s** *packet-size* | **-t** *timeout* | **-tos** *tos* | **-v** | **-vpn-instance** *vpn-instance-name*] * *remote-system*

View Any view

Parameter **ip**: Supports IPv4 protocol.

-a *source-ip*: Specifies the source IP address of an ICMP echo request. It must be a legal IP address configured on the device.

-c *count*: Specifies the number of times that an ICMP echo request is sent, in the range 1 to 4294967295. The default value is 5.

-f: Discards packets larger than the MTU of a given interface, that is, the ICMP echo request is not allowed to be fragmented.

-h *ttl*: Specifies the TTL value for an ICMP echo request, in the range 1 to 255. The default value is 255.

-i *interface-type interface-number*: Specifies the ICMP echo request sending interface by its type and number.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMP echo response, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-n: Specifies that the Domain Name System (DNS) is disabled. DNS is enabled by default, that is, the *hostname* is translated into an address.

-p *pad*: Specifies the padded bytes in an ICMP echo request, in hexadecimal format. For example, if *pad* is configured as ff, then the packets will be padded with ff. By default, the padded bytes start from 0x01 up to 0xff where another round starts again if necessary.

-q: Presence of this parameter indicates that only statistics are displayed. By default, all information is displayed.

-r: Records routes. By default, routes are not recorded.

-s *packet-size*: Specifies length (in bytes) of an ICMP echo request, in the range 20 to 8100. The default value is 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMP echo request, in the range 0 to 65535. It defaults to 2000.

-tos *tos*: Specifies type of service (ToS) of an echo request, in the range 0 to 255. The default value is 0.

-v: Displays non ICMP echo reply received. By default, the system does not display non ICMP packets echo reply.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters. It is case sensitive.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description Use the **ping** command to verify whether the destination device in an IP network is reachable, and to display the related statistics.

Note that:

- You must use the command in the form of **ping ip** *ip* instead of **ping** *ip* if the destination name is a key word, such as **ip**.
- Only the directly connected segment address can be pinged if the outgoing interface is specified with the **-i** argument.

Example # Check whether the device with an IP address of 10.1.1.5 is reachable.

```
<Sysname> ping 10.1.1.5
PING 10.1.1.5 : 56 data bytes, press CTRL_C to break
Reply from 10.1.1.5 : bytes=56 Sequence=1 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=2 ttl=255 time = 2 ms
Reply from 10.1.1.5 : bytes=56 Sequence=3 ttl=255 time = 1 ms
Reply from 10.1.1.5 : bytes=56 Sequence=4 ttl=255 time = 3 ms
Reply from 10.1.1.5 : bytes=56 Sequence=5 ttl=255 time = 2 ms

--- 10.1.1.5 ping statistics ---
5 packet(s) transmitted
5 packet(s) received
0.00% packet loss
round-trip min/avg/max = 1/2/3 ms
```

ping ipv6

Syntax **ping ipv6** [**-a** *source-ipv6* | **-c** *count* | **-m** *interval* | **-s** *packet-size* | **-t** *timeout*] * *remote-system* [**-i** *interface-type interface-number*]

View Any view

Parameter **-a** *source-ipv6*: Specifies the source IPv6 address of an ICMP echo request. It must be a legal IPv6 address configured on the device.

-c *count*: Specifies the number of times that an ICMPv6 echo request is sent, in the range 1 to 4294967295. The default value is 5.

-m *interval*: Specifies the interval (in milliseconds) to send an ICMPv6 echo reply, in the range 1 to 65535. The default value is 200 ms.

- If a response from the destination is received within the timeout time, the interval to send the next echo request equals the actual response period plus the value of *interval.*
- If no response from the destination is received within the timeout time, the interval to send the next echo request equals the *timeout* value plus the value of *interval.*

-s *packet-size*: Specifies length (in bytes) of an ICMPv6 echo request, in the range 20 to 8100. It defaults to 56.

-t *timeout*: Specifies the timeout value (in milliseconds) of an ICMPv6 echo request, in the range 0 to 65535. It defaults to 2000.

remote-system: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.

-i *interface-type interface-number*: Specifies an outgoing interface by its type and number. This parameter can be used only in case that the destination address is the link local address and the specified outgoing interface must have a link local address (For the configuration of link local address, see "IPv6 Basics Configuration Commands" on page 829).

Description Use the **ping ipv6** command to verify whether an IPv6 address is reachable, and display the corresponding statistics.

You must use the command in the form of **ping ipv6** *ipv6* instead of **ping** *ipv6* if the destination name is an ipv6 name.

Example # Verify whether the IPv6 address 2001::1 is reachable.

```
<Sysname> ping ipv6 2001::1
  PING 2001::1 : 56  data bytes, press CTRL_C to break
  Reply from 2001::1  bytes=56 Sequence=1 hop limit=64  time = 20 ms
  Reply from 2001::1  bytes=56 Sequence=2 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=3 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=4 hop limit=64  time = 0 ms
  Reply from 2001::1  bytes=56 Sequence=5 hop limit=64  time = 0 ms

  --- 2001::1 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 0/4/20 ms
```

The "hop limit" field in this prompt information has the same meaning as the "ttl" field in the prompt information displayed by the IPv4 **ping** command, indicating the TTL value in the ICMPv6 echo request.

tracert

Syntax **tracert** [**-a** *source-ip* | **-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-vpn-instance** *vpn-instance-name* | **-w** *timeout*] * *remote-system*

View Any view

Parameter **-a** *source-ip*: Specifies the source IP address of a tracert packet. It must be a legal IP address configured on the device.

-f *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30, and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. You do not need to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535. The default value is 3.

-vpn-instance *vpn-instance-name*: Specifies the name of an MPLS VPN instance, which is a string of 1 to 31 characters.

-w *timeout*: Specifies the packet timeout time, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IP address or host name (a string of 1 to 20 characters) of the destination device.

Description Use the **tracert** command to trace the routers the packets traverse from the source to the destination device.

After having identified network failure with the **ping** command, you can use the **tracert** command to determine the failed node(s).

Output information of the **tracert** command includes IP addresses of all the routers the packets traverse from the source to the destination device. If a router times out, "* * *" will be displayed.

Example # Display the routers the packets traverse from the current device, with an IP address of 8.26.0.115, to the destination device.

```
<Sysname> tracert 18.26.0.115
traceroute to 18.26.0.115(18.26.0.115) 30 hops max,40 bytes packet,
```

```
press CTRL_C to break
1  128.3.112.1  10 ms 10 ms 10 ms
2  128.32.210.1  19 ms 19 ms 19 ms
3  128.32.216.1  39 ms 19 ms 19 ms
4  128.32.136.23  19 ms 39 ms 39 ms
5  128.32.168.22  20 ms 39 ms 39 ms
6  128.32.197.4  59 ms 119 ms 39 ms
7  131.119.2.5  59 ms 59 ms 39 ms
8  129.140.70.13  80 ms 79 ms 99 ms
9  129.140.71.6  139 ms 139 ms 159 ms
10  129.140.81.7  199 ms 180 ms 300 ms
11  129.140.72.17  300 ms 239 ms 239 ms
12  * * *
13  128.121.54.72  259 ms 499 ms 279 ms
14  * * *
15  * * *
16  * * *
17  * * *
18  18.26.0.115  339 ms 279 ms 279 ms
```

tracert ipv6

Syntax **tracert ipv6** [**-f** *first-ttl* | **-m** *max-ttl* | **-p** *port* | **-q** *packet-number* | **-w** *timeout*] * *remote-system*

View Any view

Parameter **-f** *first-ttl*: Specifies the first TTL, that is, the allowed number of hops for the first packet, in the range 1 to 255. It defaults to 1 and must be less than the maximum TTL.

-m *max-ttl*: Specifies the maximum TTL, that is, the maximum allowed number of hops for a packet, in the range 1 to 255. It defaults to 30 and must be greater than the first TTL.

-p *port*: Specifies the UDP port number of the destination device, in the range 1 to 65535. The default value is 33434. It is unnecessary to modify this parameter.

-q *packet-number*: Specifies the number of probe packets sent each time, in the range 1 to 65535, defaulting to 3.

-w *timeout*: Specifies the timeout time of the probe packets, in the range 1 to 65535, in milliseconds. The default value is 5000 ms.

remote-system: IPv6 address or host name (a string of 1 to 46 characters) of the destination device.

Description Use the **tracert ipv6** command to view the routers the IPv6 packets traverse from the source to the destination device.

Example # View the routes involved for packets to travel from the source to the destination with IPv6 address 3002::1

```
<Sysname> tracert ipv6 3002::1
 traceroute to 3002::1  30 hops max,60 bytes packet
 1 3003::1 30 ms  10 ms  10 ms
 2 3002::1 10 ms 11 ms 9 ms
```

161
SYSTEM DEBUGGING COMMANDS

debugging

Syntax **debugging** { **all** [**timeout** *time*] | *module-name* [*option*] }

undo debugging { **all** | *module-name* [*option*] }

View User view

Parameter all: All debugging functions.

timeout *time*: Specifies the timeout time for the **debugging all** command. When all debugging is enabled, the system automatically executes the **undo debugging all** command after the *time*. The value ranges from 1 to 1440, in minutes.

module-name: Module name, such as ARP or ATM. You can use the **debugging ?** command to display the current module name.

option: Specifies the debugging option for a specific module. Different modules have different debugging options in terms of their number and content. You can use the **debugging** *module-name* **?** command to display the currently supported options.

Description Use the **debugging** command to enable the debugging of a specific module.

Use the **undo debugging** command to disable the debugging of a specific module.

By default, debugging functions of all modules are disabled.

Note the following:

- This command is intended for network administrators to diagnose network failure.
- Output of the debugging information may degrade system efficiency, especially during the execution of the **debugging all** command. Therefore, use the command with caution.
- After finishing debugging, you can use the **undo debugging all** command to disable all the debugging functions.
- You must configure the **debugging, terminal debugging** and **terminal monitor** commands first to display detailed debugging information on the

terminal. For the detailed description on the **terminal debugging** and **terminal monitor** commands, refer to "terminal debugging" on page 2445 and "terminal monitor" on page 2447.

Related command: **display debugging**.

Example # Enable IP packet debugging.

```
<Sysname> debugging ip packet
```

display debugging

Syntax **display debugging** [**interface** *interface-type interface-number*] [*module-name*]

View Any view

Parameter **interface** *interface-type interface-number*: Displays the debugging settings of the specified interface, where *interface-type interface-number* represents the interface type and number.

module-name: Module name.

Description Use the **display debugging** command to display enabled debugging functions.

Related command: **debugging**.

Example # Display all enabled debugging functions.

```
<Sysname> display debugging
IP packet debugging is on
```

162 BASIC CONFIGURATION COMMANDS

clock datetime

Syntax **clock datetime** *time date*

View User view

Parameter *time*: Current time in the format of *HH:MM:SS*, where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

date: Current date in the format of *MM/DD/YYYY* or *YYYY/MM/DD*. *MM* is the month of the year in the range 1 to 12, *DD* is the day of the month that varies with months, and *YYYY* is a year in the range 2000 to 2035.

Description Use the **clock datetime** command to set the current time and date.

The current time and date of the device must be set in an environment that requires the acquisition of absolute time.

You may choose not to provide seconds when inputting the time parameters.

After the configuration takes effect, you can use the **display clock** command to view it.

Related command: **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**, **display clock**.

Example # Set the current system time to 14:10:20 08/01/2005.

```
<Sysname> clock datetime 14:10:20 08/01/2005
```

Set the current system time to 00:06 01/01/2007.

```
<Sysname> clock datetime 0:6 2007/1/1
```

clock summer-time one-off

Syntax **clock summer-time** *zone-name* **one-off** *start-time start-date end-time end-date add-time*

undo clock summer-time

View User view

Parameter *zone-name*: Name of the summer time, a string of 1 to 32 characters. It is case sensitive.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

start-date: Start date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

end-date: End date, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.

add-time: Time added to the standard time of the device, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

Description Use the **clock summer-time one-off** command to adopt summer time from the *start-time* of the *start-date* to the *end-time* of the *end-date*. Summer time adds the *add-time* to the current time of the device.

Use the **undo clock summer-time** command to cancel the configuration of the summer time.

After the configuration takes effect, you can use the **display clock** command to view it. Besides, the time of the log or debug information is the local time of which the time zone and summer time have been adjusted.

Note that:

- The time range from *start-time* in *start-date* to *end-time* in *end-date* must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.
- If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

Related command: **clock datetime**, **clock summer-time repeating**, **clock timezone**, **display clock**.

Example # For daylight saving time in abc1 between 06:00:00 on 08/01/2006 and 06:00:00 on 09/01/2006, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc1 one-off 6 08/01/2006 6 09/01/2006 1
```

clock summer-time repeating

Syntax **clock summer-time** *zone-name* **repeating** *start-time start-date end-time end-date add-time*

undo clock summer-time

View User view

Parameter *zone-name*: Name of the daylight saving time, a string of 1 to 32 characters.

start-time: Start time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

start-date: Start date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the start week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the start date is **Sunday**, **Monday, Tuesday, Wednesday, Thursday, Friday, Saturday**.

end-time: End time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

end-date: End date which can be set in two ways:

- Enter the year, month and date at one time, in the format of *MM/DD/YYYY* (months/days/years) or *YYYY/MM/DD*.
- Enter the year, month and date one by one, separated by spaces. The year ranges from 2000 to 2035; the month can be **January**, **February**, **March**, **April**, **May**, **June**, **July**, **August**, **September**, **October**, **November** or **December**; the end week can be the **first**, **second**, **third**, **fourth**, **fifth** or **last** week of the month; the end date is **Sunday**, **Monday**, **Tuesday**, **Wednesday**, **Thursday**, **Friday**, **Saturday**.

add-time: Time added to the current standard time, in the format of *HH:MM:SS* (hours/minutes/seconds). The zeros in the argument can be omitted except for indicating 0 hours.

Description Use the **clock summer-time repeating** command to adopt summer-time repeatedly.

Use the **undo clock summer-time** command to cancel the configuration of the daylight saving time.

For example, when *start-date* and *start-time* are set to 2007/6/6 and 00:00:00, *end-date* and *end-time* to 2007/10/10 and 00:00:00, and *add-time* to 01:00:00, it

specifies to adopt daylight saving time from 00:00:00 of June 6 until 00:00:00 of October 1 each year from 2007 (2007 inclusive). The daylight saving time adds one hour to the current device time.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Note that:

- The time range from "start-time" in "start-date" to "end-time" in "end-date" must be longer than one day and shorter than one year. Otherwise, the argument is considered as invalid and the configuration fails.

If the current system time is in the time range specified with this command, the system time automatically adds "add-time" after the execution of this command.

Related command: **clock datetime**, **clock summer-time one-off**, **clock timezone**, **display clock**.

Example # For the summer time in abc2 between 06:00:00 on 08/01/2007 and 06:00:00 on 09/01/2007 and from 06:00:00 08/01 to 06:00:00 on 09/01 each year after 2007, set the system clock ahead one hour.

```
<Sysname> clock summer-time abc2 repeating 06:00:00 08/01/2007 06:00
:00 09/01/2007 01:00:00
```

clock timezone

Syntax **clock timezone** *zone-name* { **add** | **minus** } *zone-offset*

undo clock timezone

View User view

Parameter *zone-name*: Time zone name, a string of 1 to 32 characters. It is case sensitive.

add: Positive offset to universal time coordinated (UTC) time.

minus: Negative offset to UTC time.

zone-offset: In the format of HH/MM/SS (hours/minutes/seconds), where *HH* is hours in the range 0 to 23, *MM* is minutes in the range 0 to 59, and *SS* is seconds in the range 0 to 59. The zeros in the argument can be omitted except for indicating 0 hours.

Description Use the **clock timezone** command to set the local time zone.

Use the **undo clock timezone** command to restore the local time zone to the default UTC time zone.

By default, the local time zone is UTC zone.

After the configuration takes effect, use the **display clock** command to view the result. The information such as log file and debug adopts the local time modified by time-zone and daylight saving time.

Related command: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **display clock**.

Example # Set the name of the local time zone to Z5, five hours ahead of UTC time.

```
<Sysname> clock timezone z5 add 5
```

command-privilege

Syntax **command-privilege level** *level* **view** *view command*

undo command-privilege view *view command*

View System view

Parameter **level** *level*: Specifies a command level in the range 0 to 3.

view *view*: Specifies a view.

command: Command to be set in the specified view.

Description Use the **command-privilege** command to assign a level for the commands in the specified view.

Use the **undo command-privilege view** command to restore the default.

By default, the commands under each view have their respective command levels. Generally, do not modify the default command levels to avoid inconvenience to your maintenance and operation.

Command privilege falls into four levels: visit, monitor, system, and manage, which are identified by 0 through 3.

The administrator can assign a privilege level for a user according to his need. When the user logs on a device, the commands available depend on the user's privilege. For example, if a user's privilege is 3 and the command privilege of VTY 0 user interface is 1, and the user logs on the system from VTY 0, he can use all the commands with privilege smaller than three (inclusive).

The following table describes the default level of the commands.

Table 622 Default level of the commands

Command level	Commands
Visit (0)	**ping**, **tracert**, **telnet**
Monitor (1)	**refresh**, **reset**, **send**
System (2)	Configuration commands

Table 622 Default level of the commands

Command level	Commands
Manage (3)	FTP, XMODEM, TFTP, file system operation commands

Example # Set the command level of the **interface** command to 0.

```
<Sysname> system-view
[Sysname] command-privilege level 0 view system interface
```

configure-user count

Syntax **configure-user count** *number*

undo configure-user count

View System view

Parameter *number*: Number of users, the value range varies with devices.

Description Use the **configure-user count** command to configure the number of users allowed to enter system view at the same time.

Use the **undo configure-user count** command to restore the default configuration.

Two users are allowed to configure in system view by default.

Related command: **display configure-user**.

- *The support for the command varies with devices.*
- *When multiple users enter system view to configure certain attribute, only the last configuration applies.*
- *When the number of users has already reached the limit, other users can not enter system view.*

Example # Configure the limit of users as 4.

```
<Sysname> system-view
[Sysname] configure-user count 4
```

display clipboard

Syntax **display clipboard**

View Any view

Parameter None

Description Use the **display clipboard** command to view the contents of the clipboard.

To copy the specified content to the clipboard:

- Move the cursor to the starting position of the content and press the <Esc+Shift+,> combination (“,” is an English comma).
- Move the cursor to the ending position of the content and press the <Esc+Shift+.> combination (“,” is an English dot) to copy the specified content to the clipboard.

Example # View the content of the clipboard.

```
<Sysname> display clipboard
---------------- CLIPBOARD-----------------
        ip route 10.1.0.0 255.0.0.0 eth 0
```

display clock

Syntax **display clock**

View Any view

Parameter None

Description Use the **display clock** command to view the current system time and date.

The current system time and date are decided by the **clock datetime**, **clock summer-time one-off** (or **clock summer-time repeating**), **clock timezone**. Refer to the *Configuring the system clock* section in the operation manual for the detailed rules.

Related command: **clock datetime**, **clock summer-time one-off**, **clock summer-time repeating**, **clock timezone**.

Example # Display the current time and date.

```
<Sysname> display clock
09:41:23 UTC Thu 12/15/2005
```

display configure-user

Syntax **display configure-user**

View Any view

Parameter None

Description Use the **display configure-user** command to display the users entering system view at the same time.

Related command: **configure-user count**.

Example # Display the users entering system view at the same time.

```
<Sysname> display configure-user
  Idx UI      Delay    Type Userlevel
+ 178 VTY 0   01:10:16 TEL  3
+ 179 VTY 1   00:00:00 TEL  3
Following are more details.
VTY 0   :
        Location: 192.168.1.59
VTY 1   :
        Location: 192.168.1.54
 +    : User-interface is active.

 F    : User-interface is active and work in async mode.
```

display current-configuration

Syntax **display current-configuration** [[**configuration** [*configuration*] | **controller** | **interface** [*interface-type*] [*interface-number*]] [**by-linenum**] [| { **begin** | **include** | **exclude** } *text*]]

View Any view

Parameter **configuration** [*configuration*]: Specifies to display non-interface configuration. If no parameter is used, all the non-interface configuration is displayed; if parameters are used, display the specified information. For example:

- **isis**: Displays the isis configuration.
- **isp**: Displays the ISP configuration.
- **post-system**: Displays the post-system configuration.
- **radius-template**: Displays the Radius template configuration.
- **system**: Displays the system configuration.
- **user-interface**: Displays the user interface configuration.

controller: Displays the controller configuration (For example CE1/PRI interface. Refer to "display controller e1" on page 205.).

interface [*interface-type*] [*interface-number*]: Displays the interface configuration, where *interface-type* indicates the interface type and *interface-number* indicates the interface number.

by-linenum: Specifies to display the number of each line.

|: Specifies to use regular expression to filter the configuration of display device.

- **begin**: Displays the configuration beginning with the specified *text*.
- **include**: Displays the configuration including the specified *text*.
- **exclude**: Displays the configuration excluding the specified *text*.

text: Regular expression in a case-insensitive string with space allowed.

Table 623 Special characters in regular expression

Character	Meaning	Note
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression "^user" matches a string begins with "user", not "Auser".
$	Ending sign, the string before it appears only at the end of a line.	Regular expression "user$" matches a string ends with "user", not "userA".
(	Left bracket, used as a stack symbol in a program	It is not recommended to user this character to establish a regular expression.
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, used to match a subexpression zero or multiple times before it	zo* can map to "z" and "zoo".
+	Addition, used to match a subexpression one or multiple times before it	zo+ can map to "zo" and "zoo", but not "z".
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

Description

Use the **display current-configuration** command to display the current validated configuration of a device.

A parameter is not displayed if it has the default configuration.

You can use the **display current-configuration** command to view the currently validated configuration. A parameter is not displayed if it has the default configuration. If the validated parameter is changed, although you have configured it, the validated parameter is displayed. For example, ip address 11.11.11.11 24 has been configured on a Loopback interface. In this case, if you execute the **display current-configuration** command, ip address 11.11.11.11 255.255.255.255 is displayed, meaning the validated subnet mask is 32 bits.

Related command:

save on page 2365, **reset saved-configuration** on page 2363, **display saved-configuration** on page 2361.

Example

Display the configuration of all controllers on the devices.

```
<Sysname> display current-configuration controller
#
```

```
controller E1 6/0
#
controller E1 6/1
 pri-set
#
controller E1 6/2
 pri-set
#
controller E1 6/3
 using e1
#
return
```

Display the configuration beginning with "user".

```
<Sysname> display current-configuration | begin user
user-interface aux 0
user-interface vty 0 4
```

display diagnostic-information

Syntax **display diagnostic-information**

View Any view

Parameter None

Description Use the **display diagnostic-information** command to display or save the statistics of each module's running status in the system.

When the system is out of order, you need to collect a lot of information to locate the problem. At this time you can use the **display diagnostic-information** command to collect prompt information of the commands **display clock**, **display version**, **display device**, **display current-configuration**.

Example # Save the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]y
Please input the file name(*.diag)[flash:/default.diag]:aa.diag
Diagnostic information is outputting to flash:/aa.diag.
Please wait...
Save succeeded.
```

You can view the content of the file aa.diag by executing the more.aa.diag command in user view, in combination of the <Page Up> and <Page Down> keys.

Display the statistics of each module's running status in the system.

```
<Sysname> display diagnostic-information
Save or display diagnostic information (Y=save, N=display)?[Y/N]n
```

display history-command

Syntax **display history-command**

View Any view

Parameter None

Description Use the **display history-command** command to display commands saved in the history buffer.

The system will save validated history commands performed last in current user view to the history buffer, which can save up to ten commands by default. You can use the **history-command max-size** command to set the size of the history buffer. Refer to "history-command max-size" on page 2460 for related configuration.

Example # Display validated history commands in current user view (the display information varies with configuration).

```
<Sysname> display history-command
  display history-command
  system-view
  vlan 2
  quit
```

display hotkey

Syntax **display hotkey**

View Any view

Parameter None

Description Use the **display hotkey** command to display hotkey information.

Example # Display hotkey information.

```
<Sysname> display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all

           =Undefined hotkeys=
Hotkeys Command
CTRL_T  NULL
CTRL_U  NULL
```

```
            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the User View.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

display this

Syntax **display this** [**by-linenum**]

View Any view

Parameter **by-linenum**: Specifies to display the number of each line.

Description Use the **display this** command to display the validated information under the current view.

After finishing a set of configurations under a view, you can use the **display this** command to check whether the configuration takes effect.

Note that:

A parameter is not displayed if it has the default configuration.

A parameter is not displayed if the configuration has not taken effect.

When you use the command under interface view, protocol view or protocol child view, the command displays the configuration corresponding to the current view.

Example # Display configuration information of the current view (the display information varies with configuration).

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] display this
#
user-interface con 0
user-interface vty 0
 history-command max-size 256
user-interface vty 1 4
#
return
```

display version

Syntax **display version**

View Any view

Parameter None

Description Use the **display version** command to view system version information.

By viewing system version information, you can learn about the current software version, rack type and the information related to the main control board and interface boards.

Example # Display system version information (The system version information varies with devices.).

```
<Sysname> display version
H3C Comware Platform Software
Comware software, Version 5.20, Beta 1202P02, Standard
Copyright(c) 2004-2006 Hangzhou Huawei-3Com Technology Co., Ltd. All
 rights reserved.
H3C MSR30-20 uptime is 0 week, 0 day, 0 hour, 17 minutes
Last reboot 2006/10/19 13:11:33
System returned to ROM By <Reboot> Command.

CPU type: FREESCALE MPC8541 833MHz
256M bytes DDR SDRAM Memory
4M bytes Flash Memory
Pcb             Version:  3.0
Logic           Version:  1.0
Basic  BootROM  Version:  2.07
Extend BootROM  Version:  2.07
[SLOT  0]CON            (Hardware)3.0,   (Driver)1.0,    (Cpld)1.0
[SLOT  0]AUX            (Hardware)3.0,   (Driver)1.0,    (Cpld)1.0
[SLOT  0]GE0/0          (Hardware)3.0,   (Driver)1.0,    (Cpld)1.0
[SLOT  0]GE0/1          (Hardware)3.0,   (Driver)1.0,    (Cpld)1.0
[SLOT  2]DSIC-9FSW      (Hardware)2.0,   (Driver)1.0,    (Cpld)1.0
[SLOT  5]FIC-8SAE       (Hardware)2.0,   (Driver)1.0,    (Cpld)2.0
[SLOT  6]FIC-2E1-F      (Hardware)0.0,   (Driver)1.0,    (Cpld)3.0
[SLOT  8]DFIC-24FSWP    (Hardware)2.0,   (Driver)1.0,    (Cpld)130.0
[SLOT 11]FIX-SNDE       (Hardware)3.0,   (Driver)2.0,    (Cpld)1.0
```

header

Syntax **header** { **incoming** | **legal** | **login** | **motd** | **shell** } *text*

undo header { **incoming** | **legal** | **login** | **motd** | **shell** }

View System view

Parameter **incoming**: Banner displayed when a user logs onto a terminal user interface by user name and password. If authentication is required, the banner is displayed after authentication.

legal: Authorization banner before login.

login: Login banner at authentication.

motd: Banner displayed before login. The support for the keyword varies with devices.

shell: Banner displayed for VTY users to enter user view.

text: Banner message, with the first character being the start and ending delimiters. After the ending delimiter is input, the system quits automatically. Refer to *Basic System Configuration* for the detailed information.

Description Use the **header** command to create a banner.

Use the **undo header** command to clear a banner.

Example # Configure a banner in user view.

```
<Sysname> system-view
[Sysname] header incoming %
Input banner text, and quit with the character '%'.
Welcome to incoming(header incoming)%
[Sysname] header legal %
Input banner text, and quit with the character '%'.
Welcome to legal (header legal)%
[Sysname] header login %
Input banner text, and quit with the character '%'.
Welcome to login(header login)%
[Sysname] header motd %
Input banner text, and quit with the character '%'.
Welcome to motd(header motd)%
[Sysname] header shell %
Input banner text, and quit with the character '%'.
Welcome to shell(header shell)%
```

- *The character % is the starting/ending character of text in this example. Entering % after the displayed text quits the header command.*
- *As the starting and ending character, % is not a part of a banner.*

Test the configuration remotely using Telnet.

```
**************************************************************************
* All rights reserved (2004-2006)                                        *
* Without the owner's prior written consent,                             *
* No decompiling or reverse-switch fabricering shall be allowed.         *
**************************************************************************

Welcome to legal(header legal)
 Press Y or ENTER to continue, N to exit.
Welcome to motd(header motd)
Welcome to login(header login)



Login authentication


Password:
Welcome to shell(header shell)

<Sysname>
```

hotkey

Syntax **hotkey** { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** } *command*

undo hotkey { **CTRL_G** | **CTRL_L** | **CTRL_O** | **CTRL_T** | **CTRL_U** }

View System view

Parameter **CTRL_G**: Assigns the hot key <Ctrl+G> to a command.

CTRL_L: Assigns the hot key <Ctrl+L> to a command.

CTRL_O: Assigns the hot key <Ctrl+O> to a command.

CTRL_T: Assigns the hot key <Ctrl+T> to a command.

CTRL_U: Assigns the hot key <Ctrl+U> to a command.

command: The command line associated with the hot key.

Description Use the **hotkey** command to assign a hot key to a command line.

Use the **undo hotkey** command to restore the default.

By default, the system specifies corresponding commands for <Ctrl+G>, <Ctrl+L> and <Ctrl+O>, while the others are null.

- <Ctrl+G> corresponds to **display current-configuration**
- <Ctrl+L> corresponds to **display ip routing-table**
- <Ctrl+O> corresponds to **undo debugging all**

You can customize this scheme as needed however.

Example # Assign the hot key <Ctrl+T> to the **display tcp status** command.

```
<Sysname> system-view
[Sysname] hotkey ctrl_t display tcp status
```

Display the configuration of hotkeys.

```
[Sysname] display hotkey
----------------- HOTKEY -----------------

            =Defined hotkeys=
Hotkeys Command
CTRL_G  display current-configuration
CTRL_L  display ip routing-table
CTRL_O  undo debug all
CTRL_T  display tcp status
           =Undefined hotkeys=
Hotkeys Command
CTRL_U  NULL

            =System hotkeys=
Hotkeys Function
CTRL_A  Move the cursor to the beginning of the current line.
CTRL_B  Move the cursor one character left.
CTRL_C  Stop current command function.
CTRL_D  Erase current character.
CTRL_E  Move the cursor to the end of the current line.
CTRL_F  Move the cursor one character right.
CTRL_H  Erase the character left of the cursor.
CTRL_K  Kill outgoing connection.
CTRL_N  Display the next command from the history buffer.
CTRL_P  Display the previous command from the history buffer.
CTRL_R  Redisplay the current line.
CTRL_V  Paste text from the clipboard.
CTRL_W  Delete the word left of the cursor.
CTRL_X  Delete all characters up to the cursor.
CTRL_Y  Delete all characters after the cursor.
CTRL_Z  Return to the user view.
CTRL_]  Kill incoming connection or redirect connection.
ESC_B   Move the cursor one word back.
ESC_D   Delete remainder of word.
ESC_F   Move the cursor forward one word.
ESC_N   Move the cursor down a line.
ESC_P   Move the cursor up a line.
ESC_<   Specify the beginning of clipboard.
ESC_>   Specify the end of clipboard.
```

quit

Syntax **quit**

View Any view

Parameter None

Description Use the **quit** command to exit to a lower-level view. If the current view is user view, the **quit** command terminates the current connection and reconnects to the device.

Example # Switch from Ethernet 1/0 interface view to system view, and then to user view.

```
[Sysname-Ethernet1/0] quit
[Sysname] quit
<Sysname>
```

return

Syntax **return**

View Any view except user view

Parameter None

Description Use the **return** command to return to user view from current view, as you do with the hot key <Ctrl+Z>.

Related command: **quit**.

Example # Return to user view from Ethernet view.

```
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] return
<Sysname>
```

super

Syntax **super** [*level*]

View User view

Parameter *level*: User level in the range 0 to 3.

Description Use the **super** command to switch from the current user level to a specified user level

There are four levels of commands:

- Visit: involves commands for network diagnosis (such as **ping** and **tracert**), commands for accessing an external device (such as Telnet client, SSH client, RLOGIN). Saving the configuration file is not allowed at this level.
- Monitor: includes the **display** and **debugging** commands for system maintenance, and service fault diagnosis. Saving the configuration file is not allowed at this level.

- System: provides service configuration commands, including routing and commands at each level of the network for providing services.
- Manage: influences the basic operation of the system and the system support modules for service support. Commands at this level involve file system, FTP, TFTP, XMODEM download and configuration file switch, power control, standby board control, user management, level setting, as well as parameter setting within a system (the last case involves those non-protocol or non RFC provisioned commands).

Login users are also classified into four levels that correspond to the four command levels. After users at different levels log in, they can only use commands at their own, or lower, levels.

Note that:

Users can switch to a lower user level unconditionally. To log in through AUX, TTY, or VTY user interface and switch to a higher user level, however, they need to enter the password (The password can be set with the **super password** command.). If the entered password is incorrect or no password is configured, the switch fails. Therefore, before switching to a higher user level, users should configure the password needed.

Related command: **super password**.

Example # Set the user level to 2 (the current user level is 3).

```
<Sysname> super 2
User privilege level is 2, and only those commands can be used
whose level is equal or less than this.
Privilege note: 0-VISIT, 1-MONITOR, 2-SYSTEM, 3-MANAGE
```

Switch the user level back to 3 (Suppose password 123 has been set; otherwise, the user level cannot be switched to 3.).

```
<Sysname> super 3
 Password:
User privilege level is 3, and only those commands can be used
whose level is equal or less than this.
```

super password

Syntax **super password** [**level** *user-level*] { **simple** | **cipher** } *password*

undo super password [**level** *user-level*]

View System view

Parameter **level** *user-level*: Specifies user level. The *user-level* argument ranges from 1 to 3 and defaults to 3.

simple: Plain text password.

cipher: Cipher text password.

password: Password, a string of characters. It is case-sensitive string.

- For simple password, it is a string of 1 to 16 characters.
- For cipher password, it is a string of 1 to 16 characters in plain text or 24 characters in cipher text. For example, the simple text "1234567" corresponds to the cipher text "(TT8F]Y5SQ=^Q'MAF4<1!!".

Description Use the **super password** command to set the password needed to switch from a lower user level to a higher one.

Use the **undo super password** command to restore the default.

By default, no password is set to switch from a lower user level to a higher one.

Note that:

- If **simple** is specified, the configuration file saves a simple password.
- If **cipher** is specified, the configuration file saves a cipher password.
- The user must always enter a simple password, no matter simple or cipher is specified.
- Cipher passwords are recommended, as simple ones are easily getting cracked.

Example # Set the password to abc in simple form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 simple abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 simple abc
```

Set the password to abc in cipher form for switching user-level to 3.

```
<Sysname> system-view
[Sysname] super password level 3 cipher abc
```

Display the password for switching user-level.

```
[Sysname] display current-configuration
#
 super password level 3 cipher =`*Y=F>*.%-a_SW8MYM2A!!
```

sysname

Syntax **sysname** sys*name*

undo sysname

View System view

Parameter *sysname*: Name of the device, a string of 1 to 30 characters.

Description Use the **sysname** command to set the name of the device.

Use the **undo sysname** demand to restore the device name to the default.

The default name varies with devices by default.

Modifying device name affects the prompt of the CLI. For example, if the device name is Sysname, the prompt of user view is <Sysname>.

Example # Set the name of the device to R2000.

```
<Sysname> system-view
[Sysname] sysname R2000
[R2000]
```

system-view

Syntax **system-view**

View User view

Parameter None

Description Use the **system-view** command to enter system view from the current user view.

Related command: **quit**, **return**.

Example # Enter system view from the current user view.

```
<Sysname> system-view
System View: return to User View with Ctrl+Z.
[Sysname]
```

163 INFORMATION CENTER CONFIGURATION COMMANDS

display channel

Syntax **display channel** [*channel-number* | *channel-name*]

View Any view

Parameter *channel-number*: Displays information of the channel with a specified number, where *channel-number* represents the channel number, in the range 0 to 9.

channel-name: Displays information of the channel with a specified name, where *channel-name* represents the channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Table 624 Information channels for different output directions

Output direction	Information channel number	Default channel name
Console	0	console
Monitor terminal	1	monitor
Log host	2	loghost
Trap buffer	3	trapbuffer
Log buffer	4	logbuffer
SNMP NMS	5	snmpagent
Log file	9	channel9

Description Use the **display channel** command to display channel information.

If no channel is specified, information for all channels is displayed.

Example # Display information for channel 0.

```
<Sysname> display channel 0
channel number:0, channel name:console
MODU_ID  NAME     ENABLE LOG_LEVEL     ENABLE TRAP_LEVEL    ENABLE DEBUG_LEVEL
ffff0000 default  Y      warnings      Y      debugging     Y      debugging
```

Table 625 Description on the fields of the display channel command

Field	Description
channel number	A specified channel number, in the range 0 to 9.

Table 625 Description on the fields of the display channel command

Field	Description
channel name	A specified channel name, which varies with user's configuration. For more information, refer to "info-center channel name" on page 2432.
MODU_ID	The ID of the module to which the information permitted through the current channel belongs
NAME	The name of the module to which the information permitted through the current channel belongs
	Default means all modules are allowed to output system information, but the module type varies with devices.
ENABLE	Indicates whether to enable or disable the output of log information, which could be Y or N.
LOG_LEVEL	The severity of log information, refer to Table 627 for details.
ENABLE	Indicates whether to enable or disable the output of trap information, which could be Y or N.
TRAP_LEVEL	The severity of trap information, refer to Table 627 for details.
ENABLE	Indicates whether to enable or disable the output of debug information, which could be Y or N.
DEBUG_LEVEL	The severity of debug information, refer to Table 627 for details.

The above information indicates to output log information with the severity from 0 to 4, trap information with the severity from 0 to 7 and debug information with the severity from 0 to 7 to the console. The source module is default.

display info-center

Syntax **display info-center**

View Any view

Parameter None

Description Use the **display info-center** command to display configurations for all channels (except channel 6 to 8) of the information center.

Example # Display configurations for all channels.

```
<Sysname> display info-center
Information Center:enabled
Log host:
    2.2.2.2, channel number : 8, channel name : channel8,
    host facility local7
Console:
    channel number : 0, channel name : console
Monitor:
    channel number : 1, channel name : monitor
SNMP Agent:
    channel number : 5, channel name : snmpagent
Log buffer:
    enabled,max buffer size 1024, current buffer size 512,
    current messages 512, dropped messages 0, overwritten messages 740
    channel number : 4, channel name : logbuffer
Trap buffer:
```

```
    enabled,max buffer size 1024, current buffer size 256,
    current messages 216, dropped messages 0, overwritten messages 0
    channel number : 3, channel name : trapbuffer
logfile:
    channel number:9, channel name:channel9
Information timestamp setting:
    log - date, trap - date, debug - date,
    loghost - date
```

Table 626 Description on the fields of the display info-center command

Field	Description
Information Center	The current state of the information center, which could be enabled or disabled.
Log host: 2.2.2.2, channel number : 8, channel name : channel8, host facility local7	The information of the log host channel (It can be displayed only when the **info-center loghost** command is configured), including IP address of the log host, the channel number(s) and channel name(s) used, and logging facility used.)
Console: channel number : 0, channel name : console	The console channel information, including the channel number(s) and channel name(s) used
Monitor: channel number : 1, channel name : monitor	The monitor channel information, including the channel number(s) and channel name(s) used
SNMP Agent: channel number : 5, channel name : snmpagent	The SNMP agent channel information, including the channel number(s) and channel name(s) used
Log buffer: enabled,max buffer size 1024, current buffer size 512, current messages 512, dropped messages 0, overwritten messages 740 channel number : 4, channel name : logbuffer	The information of the log buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
Trap buffer: enabled,max buffer size 1024, current buffer size 256, current messages 216, dropped messages 0, overwritten messages 0 channel number : 3, channel name : trapbuffer	The information of the trap buffer channel, including whether it is enabled or disabled, the maximum capacity, the current capacity, the current number of messages, the number of dropped messages, the number of messages that have been overwritten, and the channel number(s) and channel name(s) used.
logfile: channel number:9, channel name:channel9,	The logfile configurations information, including the channel number(s), channel name(s) used.
Information timestamp setting	The time stamp configurations, specifying the time stamp format for log, trap, debug, and log host information.

*Only devices that support the Logfile feature display the related logfile information after the execution of the **display info-center** command.*

display logbuffer

Syntax **display logbuffer** [**level** *severity* | **size** *buffersize*] * [| { **begin** | **exclude** | **include** } *text*]

View Any view

Parameter **level** *severity*: Displays information of the log with specified level, where *severity* represents information level, in the range 0 to 7.

Table 627 Severity description

Character	Meaning	Remarks
emergencies	0	The system is unavailable
alerts	1	Information that requires prompt reaction
critical	2	Critical information
errors	3	Error information
warnings	4	Warnings
notifications	5	Normal errors with important information
informational	6	Informational information to be recorded
debugging	7	Debugging information

size *buffersize*: Displays specified number of the latest log messages in the log buffer, where *buffersize* represents the number of the latest log messages to be displayed in the log buffer, in the range 1 to 1,024.

slot *slotnum*: Slot number.

|: The output log information filtered by a regular expression.

begin: Displays log information beginning with a specified character or string.

exclude: Displays log information that does not contain a specified character or string.

include: Displays log information that contains a specified character or string.

text: Regular expression.

Table 628 Meanings of characters in text

Character	Meaning	Remarks
^	Starting sign, the string following it appears only at the beginning of a line.	Regular expression "^user" matches a string begins with "user", not "Auser".
$	Ending sign, the string following it appears only at the end of a line.	Regular expression "user$" matches a string ends with "user", not "userA".
.	Full stop, a wildcard used in place of any character, including blank	None
*	Asterisk, used to match a subexpression before it zero or multiple times	zo* can map to "z" and "zoo".

Table 628 Meanings of characters in text

Character	Meaning	Remarks
+	Addition, used to match a subexpression before it one or multiple times	zo+ can map to "zo" and "zoo", but not "z".
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range together with [ ].	For example, "1-9" means numbers from 1 to 9 (inclusive); "a-h" means from a to h (inclusive).
[ ]	Selects one character from the group.	For example, [1-36A] can match only one character among 1, 2, 3, 6, and A.
( )	A group of characters. It is usually used with "+" or "*".	For example, (123A) means a string "123A"; "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

Description

Use the **display logbuffer** command to display the state of the log buffer and the log information recorded. Absence of the **size** *buffersize* argument indicates that all log information recorded in the log buffer is displayed.

Example

Display the state of the log buffer and the log information recorded on a device.

```
<Sysname> display logbuffer
Logging buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 718
Current messages : 512

%Jun 17 15:57:09:578 2006 Sysname IC/7/SYS_RESTART:
System restarted --
H3C Platform Software
%Jun 17 15:57:54:428 2006 Sysname DEV/5/BOARD TEMP NORMAL:
 Board temperature changes to normal in Frame 0 Slot 0, type is Sysn
ame RPU Board.
%Jun 17 15:58:00:464 2006 Sysname SHELL/5/CMD:task:CFM ip:** user:**
 command:vlan 1
%Jun 17 15:58:00:465 2006 Sysname SHELL/5/CMD:task:CFM ip:** user:**
 command:interface Aux0
```

The rest is omitted here.

Table 629 Descriptions on the fields of the display logbuffer command

Field	Description
Logging buffer configuration and contents	Indicates the current state of the log buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the log buffer, defaults to 4

Table 629 Descriptions on the fields of the display logbuffer command

Field	Description
Channel name	The channel name of the log buffer, defaults to logbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages.

display logbuffer summary

Syntax **display logbuffer summary** [**level** *severity*]

View Any view

Parameter **level** *severity*: Displays the summary of the log information of the specified level in the log buffer. *severity* represents information level, in the range 0 to 7.

Description Use the **display logbuffer summary** command to display the summary of the log buffer.

Example # Display the summary of the log buffer on a device.

```
<Sysname> display logbuffer summary
EMERG ALERT CRIT ERROR WARN NOTIF INFO DEBUG
0     0     0    0     94   0     1    0
```

Table 630 Descriptions on the fields of the display logbuffer summary command

Field	Description
EMERG	Represents emergencies, refer to Table 627 for details
ALERT	Represents alerts, refer to Table 627 for details
CRIT	Represents critical, refer to Table 627 for details
ERROR	Represents errors, refer to Table 627 for details
WARN	Represents warnings, refer to Table 627 for details
NOTIF	Represents notifications, refer to Table 627 for details
INFO	Represents informational, refer to Table 627 for details
DEBUG	Represents debugging, refer to Table 627 for details

display logfile buffer

Syntax **display logfile buffer**

View Any view

Parameter None

Description Use the **display logfile buffer** command to display contents of the log file buffer.

The support for the command varies with devices.

Example # Display the contents of the log file buffer.

```
<Sysname> display logfile buffer
%@387986%Jun 20 10:52:03 2006 Sysname %%10IC/7/SYS_RESTART:
System restarted --
H3C Platform Software
%@387988#Jun 20 10:52:48:494 2006 Sysname ENTITY/5/CPU THRESHOLD REACHED:
 Trap 1.3.6.1.4.1.2011.10.2.6.2.0.4: Entity ID is 3, cpu usage is 100%, cpu
usage threshold is 100%, admin status is 1, alarm light status is 0
%@387989#Jun 20 10:52:48:495 2006 Sysname DEV/2/BOARD TEMPERATURE NORMAL:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.15: frameIndex is 0, slotIndex 0.0
%@387990%Jun 20 10:52:48:495 2006 Sysname DEV/5/BOARD TEMP NORMAL:
```

The rest is omitted here.

display logfile summary

Syntax **display logfile summary**

View Any view

Parameter None

Description Use the **display logfile summary** command to display the configuration of the log file.

Example # Display the configuration of the log file.

```
[Sysname]display logfile summary
  Log file is enabled.
  Channel number : 9
  Log file size quota : 0 MB (0 for unlimited)
  Log file directory : cf:/logfile
  Writing frequency : 0 hour 0 min 10 sec
```

Table 631 Descriptions on the fields of the display logfile summary command

Field	Description
Log file is	The current state of a log file, which could be enabled or disabled.
Channel number	The channel number of a log file, defaults to 9.
Log file size quota	The maximum storage space reserved for a log file
Log file directory	Log file directory
Writing frequency	Log file writing frequency

display trapbuffer

Syntax **display trapbuffer** [**size** *buffersize*]

View Any view

Parameter **size** *buffersize*: Displays specified number of the latest trap messages in a trap buffer, where *buffersize* represents the number of the latest trap messages in a trap buffer, in the range 1 to 1,024.

Description Use the **display trapbuffer** command to display the state and the trap information recorded.

Absence of the **size** *buffersize* argument indicates that all trap information is displayed.

Example # Display the state of the trap buffer and the trap information recorded.

```
<Sysname> display trapbuffer
Trapping buffer configuration and contents:enabled
Allowed max buffer size : 1024
Actual buffer size : 256
Channel number : 3 , channel name : trapbuffer
Dropped messages : 0
Overwritten messages : 0
Current messages : 1

#Dec 31 14:01:25 2004 Sysname DEV/2/LOAD FINISHED:
 Trap 1.3.6.1.4.1.2011.2.23.1.12.1.20: frameIndex is 0, slotIndex 0.4
```

Table 632 Descriptions on the fields of the display trapbuffer command

Field	Description
Trapping buffer configuration and contents	Indicates the current state of the trap buffer and its contents, which could be enabled or disabled.
Allowed max buffer size	The maximum buffer size allowed
Actual buffer size	The actual buffer size
Channel number	The channel number of the trap buffer, defaults to 3
Channel name	The channel name of the trap buffer, defaults to trapbuffer
Dropped messages	The number of dropped messages
Overwritten messages	The number of overwritten messages (when the buffer size is not big enough to hold all messages, the latest messages overwrite the old ones).
Current messages	The number of the current messages.

info-center channel name

Syntax **info-center channel** *channel-number* **name** *channel-name*

undo info-center channel *channel-number*

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, a string of 1 to 30 characters. It should not start with a number, an underscore (-), a forward slash (/), or a backward slash (). The channel name is not case sensitive.

Description Use the **info-center channel name** command to name a channel with a specified channel number.

Use the **undo info-center channel** command to restore the default name for a channel with a specified channel number.

Refer to Table 624 for details of default channel names and channel numbers.

Example # Name channel 0 as abc.

```
<Sysname> system-view
[Sysname] info-center channel 0 name abc
```

info-center console channel

Syntax **info-center console channel** { *channel-number* | *channel-name* }

undo info-center console channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center console channel** command to specify the channel to output system information to the console.

Use the **undo info-center console channel** command to restore the default output channel to the console.

By default, output of information to the console is enabled with channel 0 as the default channel (known as console).

Note that the **info-center console channel** command takes effect only after the information center is enabled first with the **info-center enable** command.

Example # Set channel 0 to output system information to the console.

```
<Sysname> system-view
[Sysname] info-center console channel 0
```

info-center enable

Syntax **info-center enable**

undo info-center enable

View System view

Parameter None

Description Use the **info-center enable** command to enable information center.

Use the **undo info-center enable** command to disable the information center.

The system outputs information to the log host or the console only after the information center is enabled first.

By default, the information center is enabled.

Example # Enable the information center.

```
<Sysname> system-view
[Sysname] info-center enable
% Information center is enabled
```

info-center logbuffer

Syntax **info-center logbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center logbuffer [**channel** | **size**]

View System view

Parameter *buffersize*: Specifies the maximum number of log messages in a log buffer, in the range 0 to 1,024 with 512 as the default value.

channel-number: A specified channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center logbuffer** command to enable information output to a log buffer and set the corresponding parameters.

Use the **undo info-center logbuffer** command to disable information output to a log buffer.

By default, information output to the log buffer is enabled with channel 4 (logbuffer) as the default channel and a maximum buffer size of 512.

Note that the **info-center logbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Enable the system to output information to the log buffer with a default buffer size of 50.

```
<Sysname> system-view
[Sysname] info-center logbuffer size 50
```

info-center logfile enable

Syntax **info-center logfile enable**

undo info-center logfile enable

View System view

Parameter None

Description Use the **info-center logfile enable** command to enable the output of system information to the log file.

Use the **undo info-center logfile enable** command to disable the output of system information to the log file.

By default, the output of system information to the log file is enabled.

The support for the command varies with devices.

Example # Enable the log file feature.

```
<Sysname> system-view
[Sysname] info-center logfile enable
```

info-center logfile frequency

Syntax **info-center logfile frequency** *freq-sec*

undo info-center logfile frequency

View System view

Parameter *freq-sec*: Frequency with which the system saves the log file, in the range 1 to 86,400 seconds. The value is with devices.

Description Use the **info-center logfile frequency** command to configure the frequency with which the system saves the log file.

Use the **undo info-center logfile frequency** command to restore the default frequency.

By default, the frequency with which the system saves the log file varies with devices.

The support for the command varies with devices.

Example # Configure the frequency with which the system saves the log file as 60,000 seconds.

```
<Sysname> system-view
[Sysname] info-center logfile frequency 60000
```

info-center logfile size-quota

Syntax **info-center logfile size-quota** *size*

undo info-center logfile size-quota

View System view

Parameter *size:* The maximum capacity of a disk, in MB, the default range varies with devices. The value, however, cannot be smaller than 1MB and larger than 10 MB.

Description Use the **info-center logfile size-quota** command to set the maximum storage space reserved for a log file.

Use the **undo info-center logfile size-quota** command to restore the default maximum storage space reserved for a log file.

By default, the storage space reserved for a log file varies with devices.

The support for the command varies with devices.

Example # Set the maximum storage space reserved for a log file to 6 MB.

```
<Sysname> system-view
[Sysname] info-center logfile size-quota 6
```

info-center logfile switch-directory

Syntax **info-center logfile switch-directory** *dir-name*

View System view

Parameter *dir-name*: The name of the directory where a log file is saved, a string of 1 to 64 characters.

Description Use the **info-center logfile switch-directory** command to configure the directory where a log file is saved. For a device supporting CF partition, the directory to save a log file is the logfile directory in the second partition (cf1:) of the storage device. Ensure that the directory is created first before saving a log file into it.

By default, the directory to save a log file is the logfile directory under the root directory of the storage device.

Note that this command can be used to manually configure the directory to which a log file can be saved. The configuration will lose after system restarts or primary/backup switchover.

Example # Create a directory with the name test under cf root directory.

```
<Sysname> mkdir test
%Created dir cf:/test.
```

Set the directory to save the log file to cf:/test.

```
<Sysname> system-View
[Sysname] info-center logfile switch-directory cf:/test
```

info-center loghost

Syntax **info-center loghost** *host-ip* [**channel** { *channel-number* | *channel-name* } **facility** *local-number*] *

undo info-center loghost *host-ip*

View System view

Parameter *host-ip*: The IP address of the log host.

channel: Specifies the channel through which system information can be output to the log host.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

facility *local-number*: The logging facility of the log host The value can be local0 to local7 and defaults to local7.

Description Use the **info-center loghost** command to specify a log host and to configure the related parameters.

Use the **undo info-center loghost** command to restore the default configurations on a log host.

By default, output of system information to the log host is disabled. When it is enabled, the default channel name will be loghost and the default channel number will be 2.

Note that:

- The **info-center loghost** command takes effect only after the information center is enabled with the **info-center enable** command.
- Ensure that the IP address input is correct while using the **info-center loghost** command to configure the IP address for a log host. System will prompt an invalid address if the loopback address (127.0.0.1) is input.
- A maximum number of 4 hosts (different) can be designated as the log host.

Example # Set to output log information to a Unix station with the IP address being 1.1.1.1/16.

```
<Sysname> system-view
[Sysname] info-center loghost 1.1.1.1
```

info-center loghost source

Syntax **info-center loghost source** *interface-type interface-number*

undo info-center loghost source

View System view

Parameter *interface-type interface-number*: Specifies a source interface by its type and number.

Description Use the **info-center loghost source** command to configure the source interface to output log information to the log host.

Use the **undo info-center loghost source** command to remove the source interface to output log information to the log host.

By default, no source interface is configured to output log information to the log host, and the system selects an interface as the source interface.

Note that the **info-center loghost source** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Configure the interface Serial 1/0 as the source interface to output log information to the log host.

```
<Sysname> system-view
[Sysname] info-center loghost source serial 1/0
```

info-center monitor channel

Syntax **info-center monitor channel** { *channel-number* | *channel-name* }

undo info-center monitor channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center monitor channel** command to configure the channel to output system information to the monitor.

Use the **undo info-center monitor channel** command to restore the default channel to output system information to the monitor.

By default, output of system information to the monitor is enabled with a default channel name of monitor and a default channel number of 1.

Note that the **info-center monitor channel** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Set to output system information to the monitor through channel 0.

```
<Sysname> system-view
[Sysname] info-center monitor channel 0
```

info-center snmp channel

Syntax **info-center snmp channel** { *channel-number* | *channel-name* }

undo info-center snmp channel

View System view

Parameter *channel-number*: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center snmp channel** command to configure the channel to output system information to the SNMP NMS.

Use the **undo info-center snmp channel** command to restore the default channel to output system information to the SNMP NMS.

By default, output of system information to the SNMP NMS is enabled with a default channel name of snmpagent and a default channel number of 5.

For more information, refer to the **display snmp-agent** commands in "SNMP Configuration Commands" on page 2329.

Example # Set to output system information to the SNMP NMS through channel 6.

```
<Sysname> system-view
[Sysname] info-center snmp channel 6
```

info-center source

Syntax **info-center source** { *module-name* | **default** } **channel** { *channel-number* | *channel-name* } [**debug** { **level** *severity* | **state** *state* } * | **log** { **level** *severity* | **state** *state* } * | **trap** { **level** *severity* | **state** *state* } *] *

undo info-center source { *module-name* | **default** } **channel** { *channel-number* | *channel-name* }

View System view

Parameter *module-name*: Specifies the output rules of the system information of the specified modules, which vary with devices. For instance, if information on ARP module is to be output, you can configure this argument as ARP.

default: Specifies the output rules of the system information of all the modules allowed to output the system information. This configuration varies with devices.

debug: Debug information.

log: Log information.

trap: Trap information.

level *severity*: Specifies the severity of system information, refer to Table 627 for details.

state *state*: Specifies the state of system information, which could be **on** or **off**.

channel-number: Specifies a channel number, in the range of 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center source** command to specify the output rules of the system information.

Use the **undo info-center source** command to remove the specified output rules.

By default, the output rules for the system information are listed in Table 633.

This command can be used to filter and redirect system information.

For example, the user can set to output log information with severity higher than warnings to the log host, and information with severity higher than informational to the log buffer. The user can also set to output trap information of the IP module to a specified output direction.

Note that:

- If you do not use the *module-name* argument to set output rules for a module, the module uses the default output rules or the output rules set by the **default** keyword; otherwise the module uses the output rules separately set for it.
- When you use the *module-name* argument to separately set the output rules for a module, the default output rules for the module become: Log and trap information is enabled, with severity being informational; debug information is disabled, with severity being debugging.
- After you separately set the output rules for a module, you must use the *module-name* argument to modify or remove the rules. The new configuration by using the **default** keyword is invalid on the module.

Table 633 Default output rules for different output directions

		LOG		TRAP		DEBUG	
Output direction	**Modules allowed**	**Enabled/ disabled**	**Severity**	**Enabled/ disabled**	**Severity**	**Enabled/ disabled**	**Severity**
Console	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Monitoring terminal	default (all modules)	Enabled	warnings	Enabled	debugging	Enabled	debugging
Log host	default (all modules)	Enabled	informational	Enabled	debugging	Disabled	debugging
Trap buffer	default (all modules)	Disabled	informational	Enabled	warnings	Disabled	debugging
Log buffer	default (all modules)	Enabled	warnings	Disabled	debugging	Disabled	debugging
SNMP NMS	default (all modules)	Disabled	debugging	Enabled	warnings	Disabled	debugging
Log file	default (all modules)	Enabled	debugging	Enabled	debugging	Disabled	debugging

Example # Set the output channel for the log information of VLAN module to snmpagent and to output information with severity being emergencies.

```
<Sysname> system-view
[Sysname] info-center source vlan channel snmpagent log level emergencies
```

info-center synchronous

Syntax **info-center synchronous**

undo info-center synchronous

View System view

Parameter None

Description Use the **info-center synchronous** command to enable synchronous information output.

Use the **undo info-center synchronous** command to disable the synchronous information output.

By default, the synchronous information output is disabled.

- *Under the current command line prompt, if the user's input is interrupted by system output such as log information, then after the completion of system output the system will not display command line prompt.*
- *When users need to input some interactive information (non Y/N confirmation information) if the user's input is interrupted by system information, then after the completion of system output the system will not display command line prompt but just print the user's input.*

Example # Enable synchronous information output.

```
<Sysname> system-view
[Sysname] info-center synchronous
% Info-center synchronous output is on
```

The user receives trap messages when he/she is about to display the configurations for an Ethernet interface by inputting the **display interface ethe** command. After the system has finished its output of trap messages, it will display the user's original input, which is "display interface ethe" in this case.

```
<Sysname> system-view
[Sysname] display interface ethe
%Apr 29 08:12:44:71 2007 AR29.43 IFNET/4/LINK UPDOWN:
 Ethernet2/1: link status is UP
[Sysname] display interface ethe
```

info-center timestamp

Syntax **info-center timestamp** { **debugging** | **log** | **trap** } { **boot** | **date** | **none** }

undo info-center timestamp { **debugging** | **log** | **trap** }

View System view

Parameter **debugging**: Sets the timestamp format of the debugging information.

log: Sets the timestamp output format of the log information.

trap: Sets the timestamp output format of the trap information.

boot: The time taken to boot up the system, in the format of xxxxxx.yyyyyy, in which xxxxxx represents the most significant 32 bits of the time taken to boot up the system (in milliseconds) whereas yyyyyy is the least significant 32 bits.

date: The current system date and time, in the format of "Mmm dd hh:mm:ss:sss yyyy".

- Mmm: The abbreviations of the months in English, which could be Jan, Feb, Mar, Apr, May, Jun, Jul, Aug, Sep, Oct, Nov, or Dec.
- dd: The date, starting with a space if less than 10, for example "7".
- hh:mm:ss:sss: The local time, with hh ranging from 00 to 23, mm and ss ranging from 00 to 59, and sss ranging from 0 to 999.
- yyyy: Represents the year.

none: Indicates no time information is provided.

Description Use the **info-center timestamp** command to configure the time stamp format.

Use the **undo info-center timestamp** command to restore the default.

By default, the time stamp format for log, trap and debug information is **date**.

Example # Configure the time stamp for debug information as boot.

```
<Sysname> system-view
[Sysname] info-center timestamp debugging boot
```

info-center timestamp loghost

Syntax **info-center timestamp loghost** { **date** | **no-year-date** | **none** }

undo info-center timestamp loghost

View System view

Parameter **date**: Indicates the current system date and time, the format of which depends on the log host.

no-year-date: Indicates the current system date and time (year exclusive).

none: Indicates that no time stamp information is provided.

Description Use the **info-center timestamp loghost** command to configure the time stamp format of the log information sent to the log host.

Use the **undo info-center timestamp loghost** command to restore the default.

By default, the time stamp format for log information sent to the log host is **date.**

Example # Set not to include the year information in the output information to the log host.

```
<Sysname> system-view
[Sysname] info-center timestamp loghost no-year-date
```

info-center trapbuffer

Syntax **info-center trapbuffer** [**channel** { *channel-number* | *channel-name* } | **size** *buffersize*] *

undo info-center trapbuffer [**channel** | **size**]

View System view

Parameter **size** *buffersize*: Specifies the maximum number of trap messages in a trap buffer in the range 0 to 1,024 with 256 as the default value.

channel-number: Specifies a channel number, in the range 0 to 9.

channel-name: Specifies a channel name, which could be a default name or one that is defined by the user. The user needs to specify a channel name first before using it as a self-defined channel name. For more information, refer to "info-center channel name" on page 2432.

Description Use the **info-center trapbuffer** command to enable information output to the trap buffer and set the corresponding parameters.

Use the **undo info-center trapbuffer** command to disable information output to the trap buffer.

By default, information output to the trap buffer is enabled with channel 3 (trapbuffer) as the default channel and a maximum buffer size of 256.

Note that the **info-center trapbuffer** command takes effect only after the information center is enabled with the **info-center enable** command.

Example # Enable system to output information to the trap buffer with a default buffer size of 30.

```
<Sysname> system-view
[Sysname] info-center trapbuffer size 30
```

logfile save

Syntax **logfile save**

View Any view

Parameter None

Description Use the **logfile save** command to manually save the log buffer contents into the log file.

By default, the system automatically saves the log file based on a frequency configured by the **info-center logfile frequency** command into a directory configured by the **info-center logfile switch-directory** command.

Example # Set to manually save the log buffer contents into the log file.

```
<Sysname> logfile save
```

reset logbuffer

Syntax **reset logbuffer**

View User view

Parameter None

Description Use the **reset logbuffer** command to reset the log buffer contents.

Example # Reset the log buffer contents.

```
<Sysname> reset logbuffer
```

reset trapbuffer

Syntax **reset trapbuffer**

View User view

Parameter None

Description Use the **reset trapbuffer** command to reset the trap buffer contents.

Example # Reset the trap buffer contents.

```
<Sysname> reset trapbuffer
```

terminal debugging

Syntax **terminal debugging**

undo terminal debugging

View User view

Parameter None

Description Use the **terminal debugging** command to enable the display of debug information on the current terminal.

Use the **undo terminal debugging** command to disable the display of debug information on the current terminal.

By default, the display of debug information on the current terminal is disabled.

Note that the debug information is displayed (using the **terminal debugging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example # Enable the display of debug information on the current terminal.

```
<Sysname> terminal debugging
% Current terminal debugging is on
```

terminal logging

Syntax **terminal logging**

undo terminal logging

View User view

Parameter None

Description Use the **terminal logging** command to enable the display of log information on the current terminal.

Use the **undo terminal logging** command to disable the display of log information on the current terminal.

By default, the display of log information on the current terminal is disabled.

Note that the log information is displayed (using the **terminal logging** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example # Disable the display of log information on the current terminal.

```
<Sysname> undo terminal logging
% Current terminal logging is off
```

terminal monitor

Syntax **terminal monitor**

undo terminal monitor

View User view

Parameter None

Description Use the **terminal monitor** command to enable the monitoring of system information on the current terminal.

Use the **undo terminal monitor** command to disable the monitoring of system information on the current terminal.

- Note that the **terminal monitor** command must be configured first before the log, trap, and debug information can be displayed using the corresponding commands.
- Configuration of the **undo terminal monitor** command automatically disables the monitoring of log, trap, and debug information.

By default, the monitoring of the console is enabled and the monitoring of the terminal is disabled.

Example # Enable the monitoring of system information on the current terminal.

```
<Sysname> terminal monitor
% Current terminal monitor is on
```

terminal trapping

Syntax **terminal trapping**

undo terminal trapping

View User view

Parameter None

Description Use the **terminal trapping** command to enable the display of trap information on the current terminal.

Use the **undo terminal trapping** command to disable the display of trap information on the current terminal.

By default, the display of trap information on the current terminal is enabled.

Note that the trap information is displayed (using the **terminal trapping** command) only after the monitoring of system information is enabled on the current terminal first (using the **terminal monitor** command).

Example #Enable the display of trap information on the current terminal.

```
<Sysname> terminal trapping
% Current terminal trapping is on
```

164 USER INTERFACE CONFIGURATION COMMANDS

acl

Syntax For basic and advanced ACL, use the following commands:

acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

undo acl [**ipv6**] *acl-number* { **inbound** | **outbound** }

For layer 2 ACL, use the following commands:

acl *acl-number* **inbound**

undo acl *acl-number* **inbound**

View VTY user interface view

Parameter **ipv6**: When this keyword is present, the command supports IPv6; otherwise, it supports IPv4.

acl-number: Number of access control list, in the range 2000 to 4999, where

- 2000 to 2999 are the basic ACL number
- 3000 to 3999 are the advanced ACL number
- 4000 to 4999 are the layer 2 ACL number

inbound: Controls dial-in for a user interface.

outbound: Controls dial-out for a user interface.

Description Use the **acl** command to reference an ACL to control dial-in or dial-out of the current users.

Use the **undo acl** command to remove the ACL.

For details regarding ACL, refer to "IPv4 ACL Configuration Commands" on page 2087 and "IPv6 ACL Configuration Commands" on page 2103.

By default, dial-in and dial-out of VTY users are not restricted.

Example # Remove the restriction on outgoing calls for VTY 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] undo acl 2001 outbound
```

activation-key

Syntax **activation-key** *character*

undo activation-key

View User interface view

Parameter *character*: Shortcut key for starting terminal sessions, a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters.

Description Use the **activation-key** command to define a shortcut key for starting a terminal session.

Use the **undo activation-key** command to restore the default.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. But in fact, only the first character functions as the shortcut key. For example, if you input an ASCII code value 97, the system will use its corresponding character a as the shortcut key; if you input the string b@c, the system will use the first letter b as the shortcut key.

By default, pressing the **Enter** key starts the terminal sessions. However, if you define a new shortcut key using the **activation-key** command, the **Enter** key no longer functions. You can use the **display current-configuration** command to display the shortcut key you have defined.

*The **display current-configuration** command is not supported on the VTY user interface.*

Example # Use letter s as the shortcut key for starting terminal sessions on the Console port.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] activation-key s
```

To verify the configuration, do the following:

Exit the terminal session on the Console port.

```
[Sysname-ui-console0] return
<Sysname> quit
**************************************************************************
* All rights reserved (2004-2006)                                        *
* Without the owner's prior written consent,                             *
* No decompiling or reverse-switch fabricering shall be allowed.         *
```

```
**************************************************************************

User interface con0 is available.



Please press ENTER.

# Enter <s> at the prompt of "Please press ENTER". You will see the terminal
 session being started.
<Sysname>
%Mar  2 18:40:27:981 2005 Sysname SHELL/5/LOGIN: Console login from con0
```

auto-execute command

Syntax **auto-execute command** *command*

undo auto-execute command

View User interface view

Parameter *command*: Command to be automatically executed.

Description Use the **auto-execute command** command to specify a command to be executed automatically.

Use the **undo auto-execute command** command to disable this feature.

By default, command auto-execution is disabled.

The **auto-execute command** command is supported on all types of user interfaces except the Console port and the AUX port functioning as the console port.

Once a command is configured using the **auto-execute command** command, the system automatically executes the command when a user logs on from the interface where the command is configured. After the command is completed, the connection breaks automatically.

A good example is configuring the **auto-execute command telnet** command to let users telnet to the specified host automatically.

CAUTION: *The **auto-execute command** command may disable you from configuring the system through the terminal line to which the command is applied. Therefore, before configuring the command and saving it with the configuration (using the **save** command), make sure that you can access the system by other means to remove the configuration in case a problem occurs.*

Example # Automatically execute the **display brief interface loopback** command after a user logs on from the VTY 0 interface.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] auto-execute command display brief interface loopback
% This action will lead to configuration failure through ui-vty0-4. Are you
```

```
sure? [Y/N] ]:y
[Sysname-ui-vty0]-4]
```

Telnet to the device again, the **display brief interface loopback** command will be executed automatically before the telnet connection breaks. And the following information will be displayed:

```
**************************************************************************
All rights reserved (2004-2006)                                          *
* Without the owner's prior written consent,                             *
* No decompiling or reverse-switch fabricering shall be allowed.         *
**************************************************************************

<Sysname>
The brief information of interface(s) under route mode:
Interface            Link      Protocol-link  Protocol type    Main IP
Loop1                UP        UP(spoofing)   LOOP             --

<Sysname>
```

authentication-mode

Syntax **authentication-mode { none | password | scheme [command-authorization] }**

View User interface view

Parameter **none**: Performs no authentication.

password: Performs local password authentication.

scheme: Performs authorization and authentication of AAA. For details about AAA, refer to *"AAA Configuration Commands" on page 1913.*

command-authorization: Performs command line authorization. HWTACACS allows per-command authorization. An input command is executed only after it passes authorization. For details about HWTACACS, refer to *"HWTACACS Configuration Commands" on page 1975.*

Description Use the **authentication-mode** command to set the authentication mode when users log onto the device using the current user interface.

By default, the authentication mode is **password** for TTY (asynchronous interface), VTY, and AUX user interfaces and is **none** for Console interfaces.

Related command: **set authentication password**.

CAUTION: If you configure to adopt AAA authentication (that is, the authentication mode is scheme.), then the default user level is 0.

Example # Set that no authentication is needed when users use VTY 0 interface to log onto the device. (This mode may be insecure.)

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode none
```

Set to use password authentication when users use VTY 0 interface to log onto the device. The authentication password is 321.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode password
[Sysname-ui-vty0] set authentication password cipher 321
```

Set to use username and password authentication when users use VTY 0 interface to log onto the device. The username is 123 and the authentication password is 321.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] authentication-mode scheme
[Sysname-ui-vty0] quit
[Sysname] local-user 123
[Sysname -luser-123] password cipher 321
[Sysname -luser-123] service-type telnet level 3
```

databits

Syntax **databits** { **5** | **6** | **7** | **8** }

undo databits

View User interface view

Parameter **5**: Five data bits.

6: Six data bits.

7: Seven data bits.

8: Eight data bits.

Description Use the **databits** command to set data bits on the user interface.

Use the **undo databits** command to restore the default, or eight bits.

The command is only applicable to asynchronous serial interfaces including AUX and Console ports.

Example # Set data bits to 5.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] databits 5
```

display history-command

Syntax **display history-command**

View Any view

Parameter None

Description Use the **display history-command** command to view the valid history commands that have been executed recently.

Currently, the system can display up to 256 history commands.

Related command: **history-command max-size**.

Example # Display history commands.

```
<Sysname> display history-command
  system-view
  quit
  display current-configuration
```

display user-interface

Syntax **display user-interface** [*num1* | { **aux** | **console** | **tty** | **vty** } *num2*] [**summary**]

View Any view

Parameter *num1*: Absolute number of a user interface. The value range varies by device, and normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For TTY user interfaces, the value range varies with devices, and normally starts from 1.
- For VTY user interfaces, the value ranges from 0 to 4.

summary: Displays summary about user interfaces.

Description Use the **display user-interface** command to view information about the specified or all user interfaces.

If the **summary** keyword is absent, the command displays the type of the user interface, the absolute or relative number, the speed, the user privilege level, the authentication mode and the physical location.

If the **summary** keyword is present, the command displays all the number and type of user interfaces.

Example # Display information about user interface 0.

```
<Sysname> display user-interface 0
  Idx  Type     Tx/Rx      Modem Privi Auth  Int
+ 0    CON 0    9600       -     3     N     -
  +    : Current user-interface is active.
  F    : Current user-interface is active and work in async mode.
  Idx  : Absolute index of user-interface.
  Type : Type and relative index of user-interface.
  Privi: The privilege of user-interface.
  Auth : The authentication mode of user-interface.
  Int  : The physical location of UIs.
  A    : Authentication use AAA.
  L    : Authentication use local database.
  N    : Current UI need not authentication.
  P    : Authentication use current UI's password.
```

Table 634 Description on the fields of the display user-interface command

Field	Description
+	The current user interface is active.
F	The current user interface is active and works in asynchronous mode.
Idx	The absolute number of the user interface.
Type	The type and relative number of the user interface.
Tx/Rx	The speed of the user interface.
Modem	Whether the modem is allowed to dial in (in), dial out (out), or both (inout). By default, the character - is displayed to indicate that this function is disabled.
Privi	Indicates the command level of a user under that user interface.
Auth	The authentication mode, uses one of the following, AAA (A), current user interface password (P), local database (L), none authentication (N).
Int	The physical location of the user interfaces.

Display summary about all user interfaces.

```
<Sysname> display user-interface summary
  User interface type : [CON]
            0:X
  User interface type : [TTY]
             1:XXXX XXXX XXXX XXXX
            17:XXXX XXXX XXXX XXXX
            33:XXXX XXXX XXXX XXXX
            49:XXXX XXXX XXXX XXXX
            65:XXXX XXXX XXXX XXXX
  User interface type : [AUX]
            81:X
  User interface type : [VTY]
            82:XUXU U
    3 character mode users.      (U)
   83 UI never used.             (X)
    3 total UI in use
```

Table 635 Description on the fields of the display user-interface summary command

Field	Description
User interface type	Type of user interface (CON/TTY/AUX/VTY)
0:X	0 represents the absolute number of the user interface. X means this user interface is not used; U means this user interface is in use; the number of the character X and U indicates the total number of user interfaces.
character mode users. (U)	Number of mode users, that is, the number of character U.
UI never used. (X)	Number of user interfaces not used, that is, the number of character X.
total UIs in use	Total number of user interfaces in use.

display users

Syntax **display users** [**all**]

View Any view

Parameter **all**: Displays information about users on all user interfaces.

Description Use the **display users** command to view the user information using the device.

Use the **display users all** command to view the user information of all the user interfaces supported on the device.

Example # Display the user information of the current user interface.

```
<Sysname> display users
The user application information of the user interface(s):
  Idx UI      Delay   Type Userlevel
+ 178 VTY 0   00:00:00 TEL  3
  179 VTY 1   00:02:34 TEL  3

Following are more details.
VTY 0   :
        Location: 192.168.1.54
VTY 1   :
        Location: 192.168.1.58
+   : Current operation user.
F   : Current operation user work in async mode.
```

Table 636 Description on the fields of the display users command

Field	Description
Idx	Absolute number of the user interface
UI	The first number and the second number are respectively the absolute index and relative index of the user interface.
Delay	Interval since the last input, in the format of hh:mm:ss.
Type	User type, such as Telnet, SSH, or PAD

Table 636 Description on the fields of the display users command

Field	Description
Userlevel	User authority or level: 0 for visit, 1 for monitor, 2 for system, and 3 for manage.
+	Current user
Location	Location of the user logging from the current user interface
F	The current user works in asynchronous mode

escape-key

Syntax **escape-key** { **default** | *character* }

undo escape-key

View User interface view

Parameter *character*: Specifies the shortcut key for aborting a task, a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters.

default: Restores the default escape key combination <Ctrl+C>.

Description Use the **escape-key** command to define a shortcut key for aborting tasks.

Use the **undo escape-key** command to disable the shortcut key for aborting tasks.

You can use a single character (or its corresponding ASCII code value in the range 0 to 127) or a string of 1 to 3 characters to define a shortcut key. But in fact, only the first character functions as the shortcut key. For example, if you enter an ASCII code value 113, the system will use its corresponding character q as the shortcut key; if you input the string q@c, the system will use the first letter q as the shortcut key.

By default, you can use <Ctrl+C> to terminate a task. After defining a new shortcut key using the **escape-key** command, the new shortcut key will take the place of <Ctrl+C> to abort the task. You can use the **display current-configuration** command to display the shortcut key you have defined.

Example # Define <a> as the escape key.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] escape-key a
```

To verify the configuration, do the following:

Use the **ping** command to check the reachability of the device with the IP address of 192.168.1.49 and use the **-c** argument to specify the number of the ICMP echo packets to be sent as 20.

```
<Sysname> ping -c 20 192.168.1.49
  PING 192.168.1.49: 56  data bytes, press a to break
    Reply from 192.168.1.49: bytes=56 Sequence=1 ttl=255 time=3 ms
    Reply from 192.168.1.49: bytes=56 Sequence=2 ttl=255 time=3 ms
# Enter <a>, if the task terminates immediately and the system retur
ns to the current view, the configuration is correct.
  --- 192.168.1.49 ping statistics ---
    2 packet(s) transmitted
    2 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 3/3/3 ms

<Sysname>
```

flow-control

Syntax **flow-control** { { **hardware** [*flow-control-type1*] | **software** [*flow-control-type2*] } * | **none** }

undo flow-control

View User interface view

Parameters **hardware**: Specifies to perform hardware flow control.

software: Specifies to perform software flow control.

none: Specifies not to perform flow control.

flow-control-type1, flow-control-type2: Sets active or passive flow control. It takes the value of **in** or **out**. **in** indicates passive flow control, meaning flow on the local device is controlled by the remote device; **out** indicates active flow control, meaning the local device controls flow on the remote device. *flow-control-type1 and flow-control-type2* are mutually exclusive. For example, if *flow-control-type1* takes the value of **in**, *flow-control-type2* can only take the value of **out**.

Description Use the **flow-control** command to configure flow control mode.

Use the **undo flow-control** command to restore the default.

The default settings of this command vary with devices.

Note that:

- Support for the complete flow control function varies with devices.
- The device not supporting complete flow control does not support the *flow-control-type1* and *flow-control-type2* arguments. After this command is configured, the flow control modes for the active and passive flow control are the same.
- The device supporting complete flow control supports the *flow-control-type1* and *flow-control-type2* arguments. If neither of these two arguments are specified, the active flow control and passive flow control adopt the same

mode; if either one of these two arguments is omitted, it indicates that no flow control is performed in the direction specified by the omitted argument. For example, if you configure **flow-control hardware in**, the system automatically sets the local device not to perform flow control on the remote device.

The command is only applicable to asynchronous serial interfaces including AUX and Console ports.

Examples # Configure software flow control in user interface view (The device does not support complete flow control.).

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control software
```

Configure to adopt software mode for the active flow control and hardware mode for the passive flow control in user interface view (The device supports complete flow control.).

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control software out hardware in
```

Configure adopt software mode for both active and passive flow control in user interface view (The device supports complete flow control.).

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control software
```

Configure to adopt hardware mode for the active flow control and no flow control for the passive flow control in user interface view (The device supports complete flow control.).

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] flow-control hardware out
```

free user-interface

Syntax **free user-interface** { *num1* | { **aux** | **console** | **tty** | **vty** } *num2* }

View User view

Parameter *num1*: Absolute number of a user interface. The value range varies with devices, and normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.

- For TTY user interfaces, the value range varies with devices, and normally starts from 1.
- For VTY user interfaces, the value ranges from 0 to 4.

Description Use the **free user-interface** command to disconnect with the specified user interface.

Note that you cannot use this command to terminate your own connection.

Example # Terminate the connection with user interface VTY1.

```
<Sysname> free user-interface vty 1
Are you sure to free user-interface vty1? [Y/N]:y
<Sysname>
```

Terminate the connection with user interface VTY 0.

```
<Sysname> free user-interface vty 0
% Not allowed to clear current UI!
```

history-command max-size

Syntax **history-command max-size** *size-value*

undo history-command max-size

View User interface view

Parameter *size-value*: History buffer size in the range 0 to 256. It defaults to 10, that is, up to ten history commands can be stored.

Description Use the **history-command max-size** command to set the size of history command buffer of the current user interface.

Use the **undo history-command max-size** command to restore the default, or 10.

Example # Set the size of the history command buffer to 20.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] history-command max-size 20
```

idle-timeout

Syntax **idle-timeout** *minutes* [*seconds*]

undo idle-timeout

View User interface view

Parameter *minutes*: Specifies timeout time in minutes, in the range 0 to 35791, defaulting to 10 minutes.

seconds: Specifies timeout time in seconds, in the range 0 to 59, defaulting to 0 seconds.

Description Use the **idle-timeout** command to set the idle-timeout timer. When it expires, the user connection is terminated.

Use the **undo idle-timeout** command to restore the default.

The default idle-timeout is 10 minutes.

The system automatically terminates user's connection if there is no information interaction between the device and the user in timeout time.

Setting idle-timeout to zero disables the timer and the connection is maintained whether it is idle or not.

Example # Set the idle-timeout timer to 1 minute and 30 seconds.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] idle-timeout 1 30
```

lock

Syntax **lock**

View User view

Parameter None

Description Use the **lock** command to set a password to prevent unauthorized users from operating under the active user interface.

After entering the **lock** command, you are prompted to input a password (up to 16 characters) and then confirm it by inputting the password again. The password is successfully set only when you input the exact password during the confirmation. After setting the password, you will be required to input the password next time you enter the system.

By default, this function is disabled.

Example # Lock the active user interface.

```
<Sysname> lock
Please input password<1 to 16> to lock current user terminal interface:
Password:
Again:
```

```
                                locked !


Password:
<Sysname>
```

modem

Syntax **modem** { **both** | **call-in** | **call-out** }

undo modem { **both** | **call-in** | **call-out** }

View User interface view

Parameter **both**: Enables both dial in and dial out.

call-in: Enables dial in.

call-out: Enables dial out.

Description Use the **modem** command to enable the modem to dial in or dial out.

Use the **undo modem** command to disable this function.

By default, dial in and dial out are disabled on the modem.

This command takes effect on the AUX port and other asynchronous interfaces only, and cannot be applied to the Console port.

Example # Set the modem dial in/out attribute on TTY 1.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] modem call-in
```

modem auto-answer

Syntax **modem auto-answer**

undo modem auto-answer

View User interface view

Parameter None

Description Use the **modem auto-answer** command to set the answering mode to auto-answer.

Use the **undo modem auto-answer** command to restore the default, or manual answer.

This command takes effect on the AUX port and other asynchronous interfaces only, and cannot be applied to the Console port.

Example # Set the answering mode to auto-answer.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem auto-answer
```

modem timer answer

Syntax **modem timer answer** *time*

undo modem timer answer

View User interface view

Parameter *time*: Timeout time in the range 1 to 60 seconds.

Description Use the **modem timer answer** command to set the timeout interval spent waiting for the carrier signal after the off-hook action when setting up an incoming call connection.

Use the **undo modem timer answer** command to restore the default, or 30 seconds.

This command takes effect on the AUX port and other asynchronous interfaces only, and cannot be applied to the Console port.

Example # Set the timeout interval to 50 seconds.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] modem timer answer 50
```

parity

Syntax **parity** { **even** | **mark** | **none** | **odd** | **space** }

undo parity

View User interface view

Parameter **even**: Even parity check.

mark: Mark parity check.

none: No parity check.

odd: Odd parity check.

space: Space parity check.

Description Use the **parity** command to set the check bit of the user interface.

Use the **undo parity** command to restore the default, or **none**.

The command is only applicable to asynchronous serial interfaces including AUX and Console ports.

Example # Perform odd parity check on the AUX interface.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] parity odd
```

protocol inbound

Syntax **protocol inbound { all | pad | ssh | telnet }**

View VTY interface view

Parameter **all**: Supports all the protocols, including Telnet, SSH and PAD.

pad: Supports PAD only.

ssh: Supports SSH only.

telnet: Supports Telnet only.

Description Use the **protocol inbound** command to enable the current user interface to support either Telnet, PAD, SSH, or all of them.

By default, all the protocols are supported.

The configuration takes effect next time you log in.

CAUTION: *If SSH is configured, you must set the authentication mode to* ***scheme*** *using the* ***authentication-mode scheme*** *command to guarantee a successful login. The* ***protocol inbound ssh*** *command fails if the authentication mode is* ***password*** *or* ***none****. Related command:* ***authentication-mode****.*

By default, the authentication mode of the Telnet protocol is ***password****.*

Example # Enable the VTYs 0 through 4 to support SSH only.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] authentication-mode scheme
[Sysname-ui-vty0-4] protocol inbound ssh
```

redirect disconnect

Syntax **redirect disconnect**

View User interface view

Parameter None

Description Use the **redirect disconnect** command to manually terminate a redirected telnet connection.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute the command after using the **redirect enable** command to enable redirection on the user interface.*

Example # Manually terminate a redirected Telnet connection.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect disconnect
```

redirect enable

Syntax **redirect enable**

undo redirect enable

View User interface view

Parameter None

Description Use the **redirect enable** command to enable redirection on the active asynchronous serial interface.

Use the **undo redirect enable** command to disable this function.

By default, the redirection function is disabled.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *To use the redirection function or configure redirection-related parameters, use this command to enable redirection on the user interface.*

Related command: telnet, **display tcp statistics** on page 793.

Example # Enable redirection on user interface TTY 7.

```
<Sysname> system-view
[Sysname] user-interface tty 7
[Sysname-ui-tty7] redirect enable
```

redirect listen-port

Syntax **redirect listen-port** *port-number*

undo redirect listen-port

View User interface view

Parameter *port-number*: Number of the listening port, in the range 2000 to 50000.

Description Use the **redirect listen-port** command to specify a listening port for redirected Telnet connections.

Use the **undo redirect listen-port** command to restore the default listening port.

The default number of the listening port for redirected Telnet connections equals absolute user interface number plus 2000.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute the command after using the **redirect enable** command to enable redirection on the user interface.*

Example # Set the number of the listening port for the redirected Telnet connections to 3000.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect listen-port 3000
```

redirect refuse-negotiation

Syntax **redirect refuse-negotiation**

undo redirect refuse-negotiation

View User interface view

Parameter None

Description Use the **redirect refuse-negotiation** command to disable Telnet option negotiation when establishing redirected Telnet connection.

Use the **undo redirect refuse-negotiation** command to enable Telnet option negotiation when establishing redirected Telnet connection.

By default, Telnet option negotiation is enabled.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute the command after using the **redirect enable** command to enable redirection on the user interface.*

Example # Disable Telnet option negotiation when establishing redirected Telnet connection.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect refuse-negotiation
```

redirect return-deal from-telnet

Syntax **redirect return-deal from-telnet**

undo redirect return-deal from-telnet

View User interface view

Parameter None

Description Use the **redirect return-deal from-telnet** command to let the device that redirects Telnet connection process the carriage returns received from the Telnet client meaning to substitute 0x0d for 0x0d 0x0a and 0x0d 0x00.

Use the **undo redirect return-deal from-telnet** command to restore the default.

By default, carriage returns are not processed.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute the command after using the **redirect enable** command to enable redirection on the user interface.*

Example # Enable the device that redirects Telnet connection to process the carriage returns received from the Telnet client.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect return-deal from-telnet
```

redirect return-deal from-terminal

Syntax **redirect return-deal from-terminal**

undo redirect return-deal from-terminal

View User interface view

Parameter None

Description Use the **redirect return-deal from-telnet** command to let the device that redirects Telnet connection process the carriage returns received from the terminal (a PC connected to the console port for example), meaning to substitute 0x0d for 0x0d 0x0a and 0x0d 0x00.

Use the **undo redirect return-deal from-terminal** command to disable the device that redirects Telnet connection from processing the carriage returns.

By default, the carriage returns received from the terminal are not processed.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute other **redirect** commands after using the **redirect enable** command to enable redirection on the user interface.*

Example # Enable the device that redirects Telnet connection to process the carriage returns received from the terminal.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect return-deal from-terminal
```

redirect timeout

Syntax **redirect timeout** *time*

undo redirect timeout

View User interface view

Parameter *time*: Idle timeout in the range 30 to 86400 seconds.

Description Use the **redirect timeout** command to set the idle timeout for the redirected telnet connection. After that, the connection is terminated.

Use the **undo redirect timeout** command to allow the system to maintain an always-on redirected telnet connection.

By default, the idle timeout is 360 seconds.

- *The **redirect** commands are supported on the AUX and TTY user interfaces only.*
- *Execute the command after using the **redirect enable** command to enable redirection on the user interface.*

Example # Set the idle timeout for the redirected telnet connection to 200 seconds.

```
<Sysname> system-view
[Sysname] user-interface tty 1
[Sysname-ui-tty1] redirect timeout 200
```

screen-length

Syntax **screen-length** *screen-length*

undo screen-length

View User interface view

Parameter *screen-length*: Number of lines displayed on the next screen, in the range 0 to 512, with zero meaning to display all information at one time, that is, to disable multiple-screen output.

Description Use the **screen-length** command to set the number of lines displayed on the next screen.

Use the **undo screen-length** command to restore the default, or 24 lines.

Multiple-screen output is supported on the device. If you press <Space> when information display pauses, the system continues to display information of the next screen page. This command sets the number of lines displayed on the next screen, the displayed number of lines on the terminal, however, is decided by the specifications of the terminal. For example, you set the value of *screen-length* to 40, but the terminal can only display 24 lines. In this case, if you press <Space> when the device outputs 1 to 40 lines of information to the terminal, the current screen displays only the information from line 18 to 40. To view the first 17 lines of information, you need to press <Page Up> or <Page Down>.

Example # Set the number of lines on the Console user interface to 30.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] screen-length 30
```

send

Syntax **send** { **all** | *num1* | { **aux** | **console** | **tty** | **vty** } *num2* }

View User view

Parameter **all**: Sends messages to all user interfaces.

num1: Absolute number of a user interface. The value range varies with devices, and normally starts from 0.

num2: Relative number of a user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For TTY user interfaces, the value range varies with devices, and normally starts from 1.
- For VTY user interfaces, the value ranges from 0 to 4.

Description Use the **send** command to send messages to the specified user interface(s).

Press <Ctrl+Z> to end message input and press <Ctrl+C> to remove this operation when inputting messages.

Example # Send the message hello abc to the Console user interface.

```
<Sysname> send console 0
Enter message, end with CTRL+Z or Enter; abort with CTRL+C:
hello abc^Z
Send message? [Y/N]y
<Sysname>

***
***
***Message from con0 to con0
***
hello abc


<Sysname>
```

set authentication password

Syntax **set authentication password** { **cipher** | **simple** } *password*

undo set authentication password

View User interface view

Parameter **cipher**: Cipher text password.

simple: Plain text password.

password: A case sensitive string. If the password format is set to simple, the *password* argument must be in plain text. If it is set to cipher, *password* can be either in cipher text or in plain text depending on what has been input. A plain text password can be a string of no more than 16 consecutive characters,

1234567 for example. A cipher text password, or the encrypted version of the plain text password, comprises 24 characters, such as _(TT8F]Y5SQ=^Q'MAF4<1!!.

Description Use the **set authentication password** command to set a local authentication password.

Use the **undo set authentication password** command to remove the local authentication password.

No local authentication password is set by default.

- When setting a password, you should specify **simple** to save it in plain text in the configuration file, or specify **cipher** to save it in cipher text.
- Whether the password format is plain text or cipher text, you must type in plain text password at authentication.
- Plain text password easily gets cracked. Therefore, you are recommended to use cipher text password.

Related command: **authentication-mode**.

Example # Set the local authentication password for the user interface Console 0 to hello.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0] authentication-mode password
[Sysname-ui-console0] set authentication password cipher hello
```

After setting the password, you will be required to input the password next time you enter the system.

shell

Syntax **shell**

undo shell

View User interface view

Parameter None

Description Use the **shell** command to enable terminal services on the user interface.

Use the **undo shell** command to disable this function.

By default, terminal services are enabled on all user interfaces.

There are a few restrictions on using the **undo shell** command:

- This command is not supported on the Console port.

- This command is not supported on the AUX port if the device has only a AUX port and no Console port.
- This command cannot be used on the user interface from which you log in.

Example # Disable terminal services on the VTYs 0 through 4.

```
<Sysname> system-view
[Sysname] user-interface vty 0 4
[Sysname-ui-vty0-4] undo shell
% Disable ui-vty0-4 , are you sure ? [Y/N] y
[Sysname-ui-vty0-4]
```

The following information is displayed when a Telnet terminal logs in:

```
The connection was closed by the remote host!
```

speed (in user interface view)

Syntax **speed** *speed-value*

undo speed

View User interface view

Parameter *speed-value*: Transmission rate in bps.

The transmission rates available with asynchronous serial interfaces include:

- 300 bps
- 600 bps
- 1200 bps
- 2400 bps
- 4800 bps
- 9600 bps
- 19200 bps
- 38400 bps
- 57600 bps
- 115200 bps

Note that the transmission rate varies with devices and configuration environment.

Description Use the **speed** command to set the transmission rate on the user interface.

Use the **undo speed** command to restore the default transmission rate.

By default, the transmission rate is 9600 bps.

The command is only applicable to asynchronous serial interfaces including AUX and Console ports.

Example # Set the transmission rate on the user interface AUX 0 to 19200 bps.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] speed 19200
```

stopbits

Syntax **stopbits** { **1** | **1.5** | **2** }

undo stopbits

View User interface view

Parameter **1**: 1 stop bit.

1.5: 1.5 stop bits.

2: 2 stop bits.

Description Use the **stopbits** command to set the stop bits on the user interface.

Use the **undo stopbits** command to restore the default, or one stop bit.

The command is only applicable to asynchronous serial interfaces including AUX and Console ports.

Example # Set the stop bits on the user interface to 1.5.

```
<Sysname> system-view
[Sysname] user-interface aux 0
[Sysname-ui-aux0] stopbits 1.5
```

terminal type

Syntax **terminal type { ansi | vt100 }**

undo terminal type

View User interface view

Parameter **ansi**: Specifies the terminal display type as ANSI.

vt100: Specifies the terminal display type as VT100.

Description Use the **terminal type** command to configure the type of terminal display.

Use the **undo terminal type** command to restore the default.

By default, the terminal display type is ANSI.

Note that the system supports two types of terminal display: ANSI and VT100. If the terminal display of the device and the client (for example, hyper terminal or Telnet terminal) is inconsistent or is set to ANSI, and if the total number of the characters of the currently using command line exceeds 80, anomalies such as cursor corruption or abnormal display of the terminal display may occur on the client. Therefore, you are recommended to set the display type of both the device and the client to VT100.

Example # Set the terminal display type to VT 100.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] terminal type vt100
```

user privilege level

Syntax **user privilege level** *level*

undo user privilege level

View User interface view

Parameter *level*: Command level in the range 0 to 3.

Command level is divided into four levels of visit, monitor, system, and manage, corresponding to the number 0, 1, 2 and 3 respectively. The administrator can change the command level of a user when necessary.

Description Use the **user privilege level** command to configure the command level that the login users on the current user interface can access.

Use the **undo user privilege level** command to restore the default.

By default, the default command level is 3 for the Console user interface and 0 for other user interfaces.

Example # Set the privilege level of the user logging in from VTY 0 to 0.

```
<Sysname> system-view
[Sysname] user-interface vty 0
[Sysname-ui-vty0] user privilege level 0
```

After the user telnets to the device from VTY 0, the terminal will only display level 0 commands, as follows:

```
<Sysname> ?
User view commands:
  language-mode  Specify the language environment
  ping           Send echo messages
```

```
  quit            Exit from current command view
  super           Privilege current user a specified priority level
  telnet          Establish one TELNET connection
  tracert         Trace route function
  undo            Undo a command or set to its default status
<Sysname>
```

Enable user 1 to access level 3 commands.

```
<Sysname> system-view
[Sysname] local-user user1
New local user added.
[Sysname-luser-user1] level 3
```

user-interface

Syntax **user-interface** { *first-num1* [*last-num1*] | { **aux** | **console** | **tty** | **vty** } *first-num2* [*last-num2*] }

View System view

Parameter *first-num1*: Absolute number of the first user interface. The value range varies with devices, and normally starts from 0.

last-num1: Absolute number of the last user interface. The value range varies with devices, and normally starts from 0, but cannot be smaller than the *first-num1*.

first-num2: Relative number of the first user interface, in the following rules:

- For the AUX port, the value is 0.
- For the Console port, the value is 0.
- For TTY user interfaces, the value range varies with devices, and normally starts from 1.
- For VTY user interfaces, the value ranges from 0 to 4.

last-num2: Relative number of the last user interface, in the following rules:

- For TTY user interfaces, the value range varies with devices, and normally starts from (*first-num2*+1).
- For VTY user interfaces, the value ranges from (*first-num2*+1) to 4.

Description Use the **user-interface** command to enter a single or multiple user interface view(s).

Example # Enter Console user interface view.

```
<Sysname> system-view
[Sysname] user-interface console 0
[Sysname-ui-console0]
```

Enter the user interface view of VTY 0 to 3.

```
<Sysname> system-view
[Sysname] user-interface vty 0 3
[Sysname-ui-vty0-3]
```

165 MAC ADDRESS TABLE MANAGEMENT CONFIGURATION COMMANDS

Interfaces that MAC address table management involves can only be Layer 2 Ethernet interfaces.

display mac-address

Syntax **display mac-address blackhole** [**vlan** *vlan-id*] [**count**]

display mac-address [*mac-address* [**vlan** *vlan-id*] | [**dynamic** | **static**] [**interface** *interface-type interface-number*] [**vlan** *vlan-id*] [**count**]]

View Any view

Parameter **blackhole**: Displays blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match blackhole MAC address entries are dropped.

vlan *vlan-id*: Displays MAC address entries of the specified VLAN, where *vlan-id* is in the range 1 to 4094.

count: Displays the total number of MAC addresses in the MAC address table.

mac-address: Specifies a MAC address in the format of H-H-H.

dynamic: Displays dynamic MAC address entries. Aging time is set for these entries.

static: Displays static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

interface *interface-type interface-number*: Displays the MAC address entry of a specified interface, where *interface-type interface-number* specifies an interface by its type and number.

Description Use the **display mac-address** command to display information about the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

Example # Display the MAC address table entry for MAC address 00e0-fc01-0101.

```
<Sysname> display mac-address 00e0-fc01-0101
MAC ADDR     VLAN ID  STATE      PORT INDEX      AGING TIME(s)
00e0-fc01-0101 1   Learned   GigabitEthernet1/0  AGING
```

Table 637 Description on the fields of the display mac-address command

Field	Description
MAC ADDR	MAC address
VLAN ID	ID of the VLAN to which the MAC address belongs
STATE	State of a MAC address, which could be Config static, Config dynamic, Learned and Blackhole.
PORT INDEX	Port name (Displayed as N/A for a blackhole MAC address)
AGING TIME(s)	Aging time, which could be: AGING, indicates that the entry is aging. NOAGED, indicates that the entry does not age.

display mac-address aging-time

Syntax **display mac-address aging-time**

View Any view

Parameter None

Description Use the **display mac-address aging-time** command to display the aging time of dynamic entries in the MAC address table.

Related commands: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**, **display mac-address**.

Example # Display the aging time of dynamic entries in the MAC address table.

```
<Sysname> display mac-address aging-time
Mac address aging time: 300s
```

The above information indicates that the aging time of dynamic entries in the MAC address table is 300 seconds.

display mac-address mac-learning

Syntax **display mac-address mac-learning** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number. The MAC address learning status of the specified interface will be displayed.

Description Use the **display mac-address mac-learning** command to display MAC address learning status of the specified or all Ethernet interfaces.

Example # Display MAC address learning status of all Ethernet interfaces.

```
<Sysname> display mac-address mac-learning
Mac address learning status of the switch: enable

PortName               Learning Status
GigabitEthernet1/1       enable
GigabitEthernet1/2       enable
GigabitEthernet1/3       enable
GigabitEthernet1/4       enable
GigabitEthernet2/1       enable
GigabitEthernet2/2       enable
GigabitEthernet2/3       enable
GigabitEthernet2/4       enable
```

Table 638 Description on the fields of display mac-address mac-learning

Field	Description
Mac-address learning status of the switch	Global MAC address learning status, enabled or disabled.
PortName	Port name
Learning Status	Interface MAC address learning status, enabled or disabled.

mac-address (Ethernet interface view)

Syntax **mac-address** { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

undo mac-address { **dynamic** | **static** } *mac-address* **vlan** *vlan-id*

View Ethernet interface view

Parameter **dynamic**: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

mac-address: Specifies a MAC address in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN to which the Ethernet interface belongs. *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

Description Use the **mac-address** command to add or modify a MAC address entry on a specified Ethernet port.

Use the **undo mac-address** command to remove a MAC address entry on the Ethernet port.

Note that:

- As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic MAC address table entries however will be lost whether you save the configuration or not.
- You cannot configure a static or dynamic MAC address entry on an aggregation port.

Related command: **display mac-address**.

Example # Add a static entry for MAC address 00e0-fc01-0101 on the interface Ethernet 1/1 with VLAN ID 2.

```
<Sysname> system-view
[Sysname] interface Ethernet 1/1
[Sysname-Ethernet1/1] mac-address static 00e0-fc01-0101 vlan 2
```

mac-address (system view)

Syntax **mac-address** { **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [{ **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*]

undo mac-address [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*

undo mac-address [**dynamic** | **static**] **interface** *interface-type interface-number*

View System view

Parameter **blackhole**: Blackhole MAC address entries. These entries do not age but you can add or remove them. The packets whose destination MAC addresses match blackhole MAC address entries are dropped.

mac-address: Specifies a MAC address in the format of H-H-H.

vlan *vlan-id*: Specifies the VLAN where the Ethernet interface belongs. *vlan-id* is the specified VLAN ID, in the range 1 to 4094.

dynamic: Dynamic MAC address entries. Aging time is set for these entries.

static: Static MAC address entries. Similar to blackhole MAC address entries, these entries do not age but you can add or remove them.

interface *interface-type interface-number*: Outbound interface, with *interface-type interface-number* representing the interface type and number.

Description Use the **mac-address** command to add or modify a MAC address entry.

Use the **undo mac-address** [{ **blackhole** | **dynamic** | **static** } *mac-address* **interface** *interface-type interface-number* **vlan** *vlan-id*] command to remove one or all MAC address entries.

Use the **undo mac-address** [**blackhole** | **dynamic** | **static**] [*mac-address*] **vlan** *vlan-id* command to remove a MAC address entry, MAC address entries of a specified type, or all MAC address entries for a VLAN.

Use the **undo mac-address** [**blackhole** | **dynamic** | **static**] **interface** *interface-type interface-number* command to remove a MAC address entry, MAC address entries of a specified type, or all MAC address entries for an Ethernet port.

Use the **undo mac-address** [**blackhole** | **dynamic** | **static**] [*mac-address*] **interface** *interface-type interface-number* **vlan** *vlan-id* command to remove a MAC address entry or all MAC address entries for an Ethernet port.

Note that you can change a dynamic entry to a static or blackhole entry but not vice versa.

As your MAC address entries configuration cannot survive a reboot, save it after completing the configuration. The dynamic entries however will be lost whether you save the configuration or not.

Related command: **display mac-address**.

Example # Add a static entry for MAC address 00e0-fc01-0101. All frames destined to this MAC address are sent out of the interface Ethernet 1/1 which belongs to VLAN 2.

```
<Sysname> system-view
[Sysname] mac-address static 00e0-fc01-0101 interface ethernet 1/1 vlan 2
```

mac-address mac-learning disable

Syntax **mac-address mac-learning disable**

undo mac-address mac-learning disable

View System view, Layer 2 Ethernet interface view, aggregation port group view

Parameter **disable**: Disables MAC address learning.

Description Use the **mac-address mac-learning disable** command to disable MAC address learning globally or on a specified Ethernet interface depending on the view you entered.

Use the **undo mac-address mac-learning disable** command to enable MAC address learning globally or on a specified Ethernet interface depending on the view you entered.

By default, MAC address learning is enabled globally and on all Ethernet ports.

Note that:

- You may need to disable MAC address learning sometimes to prevent the MAC address table from being saturated, for example, when your device is being attacked by a great deal of packets with different source MAC addresses. This somewhat affects update of the MAC address table.
- As disabling MAC address learning may result in broadcast storms, you need to enable broadcast storm suppression after you disable MAC address learning on a port.

Related command: **display mac-address mac-learning**.

Example # Disable global MAC address learning.

```
<Sysname> system-view
[Sysname] mac-address mac-learning disable
```

Disable MAC address learning on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mac-address mac-learning disable
```

mac-address max-mac-count (Ethernet interface view)

Syntax **mac-address max-mac-count** { *count* | **disable-forwarding** }

undo mac-address max-mac-count [**disable-forwarding**]

View Ethernet interface view, aggregation port group view

Parameter *count*: Maximum number of MAC addresses that can be learned on a port. When the argument takes 0, the VLAN is not allowed to learn MAC addresses. The value range for this argument varies with devices.

disable-forwarding: Disables forwarding of frames with unknown destination MAC addresses after the number of learned MAC addresses reaches the upper limit.

Description Use the **mac-address max-mac-count** *count* command to configure the maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **mac-address max-mac-count disable-forwarding** command to configure whether forwarding frames with unknown destination MAC addresses is allowed after the number of learned MAC addresses reaches the upper limit.

Use the **undo mac-address max-mac-count** command to restore the default maximum number of MAC addresses that can be learned on an Ethernet port.

Use the **undo mac-address max-mac-count disable-forwarding** command to allow forwarding frames received on an Ethernet port with unknown destination MAC addresses after the number of learned MAC addresses reached the upper limit.

The default maximum number of MAC addresses that can be learned on a port varies with devices. When the upper limit is reached, frames received with unknown destination MAC addresses on a port are forwarded by default.

The command takes effect on the current port only when executed in interface view.

Related command: **mac-address (system view)**, **mac-address (Ethernet interface view)**, **mac-address timer**.

Example # Set the maximum number of MAC addresses that can be learned on port Ethernet 1/0 to 600. After this upper limit is reached, frames received with unknown destination MAC addresses on the port will not be forwarded.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] mac-address max-mac-count 600
[Sysname-Ethernet1/0] mac-address max-mac-count disable-forwarding
```

mac-address timer

Syntax **mac-address timer** { **aging** *seconds* | **no-aging** }

undo mac-address timer aging

View System view

Parameter **aging** *seconds*: Sets a aging time for dynamic MAC address entries, in the range 10 to 4080 seconds.

no-aging: Sets dynamic MAC address entries not to age.

Description Use the **mac-address timer** command to configure the aging timer for dynamic MAC address entries.

Use the **undo mac-address timer** command to restore the default value.

By default the aging timer for dynamic MAC address entries is 300 seconds.

Set the aging timer appropriately: a long aging interval may cause the MAC address table to retain outdated entries and fail to accommodate latest network changes; a short interval may result in removal of valid entries and hence unnecessary broadcasts which may affect device performance.

Example # Set the aging timer for dynamic MAC address entries to 500 seconds.

```
<Sysname> system-view
[Sysname] mac-address timer aging 500
```

166 POE CONFIGURATION COMMANDS

The support for the commands in this document varies with devices.

apply poe-profile

Syntax **apply poe-profile** { **index** *index* | **name** *profile-name* }

undo apply poe-profile { **index** *index* | **name** *profile-name* }

View PoE interface view

Parameter **index** *index*: Specifies the index number of the PoE configuration file. The index number ranges from 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file. The file name consists of 1 to 15 characters.

Description Use the **apply poe-profile** command to apply the PoE configuration file to the current PoE interface.

Use the **undo apply poe-profile** command to remove the application of the PoE configuration file to the current PoE interface.

Note that the index number, instead of the name, of the PoE configuration file will be displayed when you execute the **display this** command.

Related command: **display poe-profile** and **apply poe-profile** interface.

Example # Apply the PoE configuration file named A20 to the PoE interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] apply poe-profile name A20
[Sysname-Ethernet1/0] display this
#
interface Ethernet1/0
 port link-mode route
 apply poe-profile index 1
#
```

display poe device

Syntax **display poe device**

View Any view

Parameter None

Description Use the **display poe device** command to display the mapping between ID, module, and slot of the power sourcing equipment (PSE).

Example # Display the mapping between ID, module, and slot of each PSE. (The information displayed varies with devices.)

```
<Sysname> display poe device
 PSE ID  SlotNo PortNum  MaxPower(W)  State   Model
 5        5         24       200           on     LSBMGV48TP
 6        6         16       200           on     LSB1GV48
```

Table 639 Description on fields of the display poe device command

Field	Description
PSE ID	ID of the PSE
SlotNo	Slot number of the PSE
PortNum	Number of PoE interfaces on the PSE
MaxPower(W)	Maximum power of the PSE (W)
State	PSE state: on: The PSE is supplying power. off: The PSE stops supplying power. faulty: The PSE is faulty
Model	PSE model

display poe interface

Syntax **display poe interface** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

Description Use the **display poe interface** command to display the power information of the specified interface.

If no interface is specified, the power information of all PoE interfaces is displayed.

Example # Display the state of Ethernet 1/0.

```
<Sysname> display poe interface ethernet 1/0
 Port Power Priority               : critical
```

```
Port Operating Status              : on
Port IEEE Class                    : 1
Port Detection Status              : delivering-power
Port Power Mode                    : signal
Port Current Power              : 11592    mW
Port Average Power              : 11610    mW
Port Peak                       : 11684    mW
Port Max Power                  : 15400    mW
Port Current                       : 244      mA
Port Voltage                       : 51.7     V
Port PD Description                : IP Phone For Room 101
```

Table 640 Description on fields of the display poe interface ethernet command

Field	Description
Port Power Enabled	PoE enabled/disabled state ■ enable: PoE is enabled. ■ disable: PoE is disabled.
Port Power Priority	Power priority of the PoE interface: ■ critical (highest) ■ high ■ low
Port Operating Status	Operating state of a PoE interface: ■ off: PoE is disabled. ■ on: Power is supplied for a PoE interface normally. ■ power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. ■ power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. ■ power-itself: The external equipment is supplying power for itself. ■ power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power. ■ Different models of device support different operating states.
Port IEEE class	PD power class: 0, 1, 2, 3, 4, and - The support for the - field depends on the device model.
Port Detection Status	Power detection state of a PoE interface: ■ disabled: The PoE function is disabled. ■ searching: The PoE interface is searching for the PD. ■ delivering-power: The PoE interface is supplying power for the PD. ■ fault: There is a fault defined in 802.3af. ■ test: The PoE interface is under test. ■ other-fault: There is a fault other than defined in 802.3af. ■ pd-disconnect: The PD is disconnected. Different models of device support different detection states.

Table 640 Description on fields of the display poe interface ethernet command

Field	Description
Port Power Mode	Power mode of a PoE interface: ■ signal: Power is supplied over signal cables. ■ spare: Power is supplied over spare cables. Different models of device support different power supply modes.
Port Current Power	Current power of a PoE interface, including PD consumption power and transmission loss The transmission loss usually does not exceed one watt. The specific loss depends on the device model.
Port Average Power	Average power of a PoE interface
Port Peak Power	Peak power of a PoE interface
Port Max Power	Maximum power of a PoE interface
Port Current	Current of a PoE interface
Port Voltage	Voltage of a PoE interface
Port PD Description	Description of the PD connected to the PoE interface, which is used to identify the type and location of the PD.

Display the state of all PoE interfaces.

```
<Sysname> display poe interface
 Interface  Enable   Priority  CurPower  Operating    IEEE   Detection
                                  (W)        Status       class  Status
 GE0/1      enable   low        4.4        on           1      delivering-power
 GE0/2      enable   critical   0          on           -      disabled
 GE0/3      enable   low        0          on           -      disabled
 GE0/4      enable   critical   0          on           -      searching
 GE0/5      enable   low        4.0        on           2      delivering-power
 GE0/6      enable   low        0          on           -      disabled
 GE0/7      disable  low        0          off          -      fault
 GE0/8      disable  low        0          off          -      disabled
 GE0/9      disable  low        0          off          -      disabled
 GE0/10     disable  low        0          off          -      disabled
 GE0/11     disable  low        0          off          -      disabled
 GE0/12     disable  low        0          off          -      disabled

 ---  2 port(s) on,    8.4(W) consumed,   171.6(W) Remaining ---
```

Table 641 Description on fields of the display poe interface command

Field	Description
Interface	Shortened form of a PoE interface
Enable	PoE enabled/disabled state: ■ enable: PoE is enabled. ■ disable: PoE is disabled.
Priority	Power priority of a PoE interface: ■ critical (highest) ■ high ■ low
CurPower	Current power of a PoE interface

Table 641 Description on fields of the display poe interface command

Field	Description
Operating Status	Operating state of a PoE interface ■ off: PoE is disabled. ■ on: Power is supplied for a PoE interface normally. ■ power lack: The guaranteed remaining power of the PSE is not high enough to supply power for a critical PoE interface. ■ power-deny: The PSE refuses to supply power. The power required by the powered device (PD) is higher than the configured power. ■ power-itself: The external equipment is supplying power for itself. ■ power-limit: The PSE is supplying a limited power. The power required by the PD is higher than the configured power and the PSE still supplies the configured power. Different models of device support different operating states.
IEEE class	PD power class stipulated by IEEE
Detection Status	Power detection state of a PoE interface: ■ disabled: The PoE function is disabled. ■ searching: The PoE interface is searching for the PD. ■ delivering-power: The PoE interface is supplying power for the PD. ■ fault: There is a fault defined in 802.3af. ■ test: The PoE interface is under test. ■ There is a fault other than defined in 802.3af. ■ pd-disconnect: The PD is disconnected. Different models of device support different power detection states.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power consumed by the current PoE interface
Remaining	Total remaining power of the system

display poe interface power

Syntax **display poe interface power** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Specifies an interface by its type and number.

Description Use the **display poe interface power** command to display the power information of a PoE interface(s).

If no interface is specified, the power information of all PoE interfaces is displayed.

Example # Display the power information of Ethernet 1/0.

```
<Sysname> display poe interface power ethernet 1/0
Interface  CurPower PeakPower MaxPower PD Description
             (W)        (W)        (W)
 Eth1/0    15.0       15.3       15.4      Acess Point on Room 509 for Peter
```

Display the power information of all PoE interfaces.

```
<Sysname> display poe interface power
Interface  CurPower PeakPower MaxPower PD Description
             (W)        (W)       (W)
 GE2/25    4.4        4.5       4.6         IP Phone on Room 309 for Peter....
 GE2/26    4.4        4.5       15.4        IP Phone on Room 409 for Peter Pan
 GE2/27    15.0       15.3      15.4       Acess Point on Room 509 for Peter
 GE2/28    0          0           0          IP Phone on Room 609 for Peter....
 GE2/29    0          0           0          IP Phone on Room 709 for Jack
 GE2/30    0          0           0          IP Phone on Room 809 for Alien

---  3 port(s) on,   23.8(W) consumed,   776.2(W) Remaining ---
```

Table 642 Description on fields of the display poe interface power command

Field	Description
Interface	Shortened form of a PoE interface
CurPower	Current power of a PoE interface
PeakPower	Peak power of a PoE interface
MaxPower	Maximum power of a PoE interface
PD Description	Description of the PD connected with a PoE interface When the description contains more than 34 characters, the first 30 characters followed by four dots will be displayed.
port(s) on	Number of PoE interfaces that are supplying power
consumed	Power currently consumed by all PoE interfaces
Remaining	Total remaining power of the system

display poe power-usage

Syntax **display poe power-usage**

View Any view

Parameter None

Description Use the **display poe power-usage** command to display the power information of the PoE power and all PSEs.

Example # Display the power information of the PoE power and all PSEs.

```
<Sysname> display poe power-usage
PoE Current Power                : 600   W
PoE Max Power                     : 2000  W
PoE Max Guaranteed Power         : 1000  W
PoE Remaining Allocate Power    : 800   W
PoE Remaining Guaranteed Power  : 600   W
PoE Total Powered Port Number   : 60
Detailed power usage of PSE(s):
PSE ID   Max    Current    Peak    Average    Remaining     Powered
         (W)     (W)         (W)     (W)         Guaranteed(W)      PortNum
1        300     200         230     205         100                  20
2        400     300         345     290         200                  30
4        500     100         120     110         300                  10
```

Table 643 Description on fields of the display poe power-usage command

Field	Description
PoE Current Power	Total consumption power of the PSE
PoE Max Power	Maximum PoE power
PoE Max Guaranteed Power	Guaranteed maximum PoE power, namely, the maximum power supplied to critical PSEs.
PoE Remaining Allocate Power	Remaining allocable PoE power = Maximum PoE power - the sum of the maximum power of all PoE-enabled PSEs
PoE Remaining Guaranteed Power	Guaranteed remaining PoE power = Guaranteed maximum PoE power - the sum of the maximum power of critical PSEs
PoE Total Powered Port Number	Number of PoE interfaces that are currently supplying power
PSE ID	ID of the PSE
Max	Maximum power of the PSE
Current	Current power of the PSE
Peak	Peak power of the PSE
Average	Average power of the PSE
Remaining Guaranteed	Guaranteed remaining power of the PSE = Guaranteed maximum power of the PSE - the sum of the maximum power of critical PoE interfaces of the PSE
Powered PortNum	Number of PoE interfaces to which the PSE is supplying power

display poe pse

Syntax **display poe pse** [*pse-id*]

View Any view

Parameter *pse-id*: PSE ID. You can use the **display poe device** command to view the mapping between PSE ID and slot. If you enter a PSE ID, the information of the PSE is displayed. Otherwise, the information of all PSEs on the device will be displayed.

pse-id indicates number of the slot where a PoE interface locates.

Description Use the **display poe pse** command to display the information of the specified PSE.

Example # Display the information of PSE 6.

```
<Sysname> display poe pse 6
 PSE ID                            : 6
 PSE Slot No                       : 6
 PSE Model                         : LSBMPOEGV48TP
 PSE Power Enabled                 : enable
 PSE Power Preempted               : no
 PSE Power Priority                : low
 PSE Current Power                 : 130      W
```

```
PSE Average Power                 : 20       W
PSE Peak Power                     : 240      W
PSE Max Power                      : 200      W
PSE Remaining Guaranteed          : 120      W
PSE CPLD Version                   : 100
PSE Software Version              : 200
PSE Hardware Version              : 100
PSE Legacy Detection              : disable
PSE Utilization-threshold         : 80
PSE Pse-policy Mode                : disable
PSE Pd-policy Mode                 : disable
PSE PD Disconnect Detect Mode     : DC
```

Table 644 Description on fields of the display poe pse command

Field	Description
PSE ID	ID of the PSE
PSE Slot No	Slot number of the PSE
PSE Model	Model of the PSE module
PSE Power Enabled	PoE is enabled for the PSE
PSE Power Preempted	PSE power preempted state ■ no: The power of the PSE is not preempted. ■ yes: The power of the PSE is preempted so that it can supply power, although PoE is enabled for the PSE.
PSE Power Priority	Power priority of the PSE
PSE Current Power	Current power of the PSE
PSE Average Power	Average power of the PSE
PSE Peak Power	Peak power of the PSE
PSE Max Power	Maximum power of the PSE
PSE Remaining Guaranteed	Guaranteed remaining power of the PSE = Maximum power of the PSE- the sum of the maximum power of the critical PoE interfaces of the PSE
PSE CPLD Version	PSE CPLD version
PSE Software Version	PSE software version number
PSE Hardware Version	PSE hardware version number
PSE Legacy Detection	Nonstandard PD detection by the PSE: ■ enable: Enabled ■ disable: Disabled
PSE Utilization-threshold	PSE power alarm threshold
PSE Pse-policy Mode	PSE power management policy mode
PSE Pd-policy Mode	PD power management policy mode
PSE PD Disconnect Detect Mode	PD disconnection detection mode

display poe-power

Syntax **display poe-power**

View Any view

Parameter None

Description Use the **display poe-power** command to display the information of the PoE power.

Example # Display information of the PoE power.

```
<Sysname> display poe-power
 PoE Current Power           : 1870     W
 PoE Average Power           : 2100     W
 PoE Peak Power              : 2350     W
 PoE Max Power               : 2000     W
 PoE Nominal Power           : 2500     W
 PoE Current Current         : 3.00     A
 PoE Current Voltage         : 55.00    V
 PoE Input-threshold Lower   : 111.22   V
 PoE Input-threshold Upper   : 131.00   V
 PoE Output-threshold Lower  : 45.00    V
 PoE Output-threshold Upper  : 57.00    V
 PoE Hardware Version        : 0002
 PoE Software Version        : 0001
 PoE Power Number            : 2
 PoE Power 1:
     Manufacturer            : Tyco Electronics Com
     Type                    : PSE2500-A
     Status                  : Normal
 PoE Power 2:
     Manufacturer            : Tyco Electronics Com
     Type                    : PSE2500-B
     Status                  : Normal
```

Table 645 Description on fields of the display poe-power command

Field	Description
PoE Current Power	Current PoE power
PoE Average Power	Average PoE power
PoE Peak Power	Peak PoE power
PoE Max Power	Maximum PoE power
PoE Nominal Power	Nominal PoE power
PoE Current Current	Current PoE current
PoE Current Voltage	Current PoE voltage
PoE Input-threshold Lower	AC input under-voltage threshold
PoE Input-threshold Upper	AC input over-voltage threshold
PoE Output-threshold Lower	DC output under-voltage threshold
PoE Output-threshold Upper	DC output over-voltage threshold
PoE Hardware Version	PoE hardware version number
PoE Software Version	PoE software version number
PoE Power Number	Number of PoE power supply units
PoE Power Manufacturer	Manufacturer of the PoE power
PoE Power Type	Type of the PoE power

Table 645 Description on fields of the display poe-power command

Field	Description
PoE Power Status	PoE power state: ■ Normal ■ Absent ■ Off ■ Master ■ Slave ■ Balance ■ Redundant ■ Alarm ■ Faulty The PoE power state varies with devices.

display poe-profile

Syntax **display poe-profile** [**index** *index* | **name** *profile-name*]

View Any view

Parameter **index** *index*: Specifies the index number of the PoE configuration file. The index number ranges from 1 to 100.

name *profile-name*: Specifies the name of the PoE configuration file. The file name consists of 1 to 15 characters.

Description Use the **display poe-profile** command to display all information of the configurations and applications of the PoE configuration file.

If no argument is specified, all information of the configurations and applications of existing PoE configuration files will be displayed.

Example # Display all information of the configurations and applications of the current PoE configuration file.

```
<Sysname> display poe-profile
Poe-profile       Index  ApplyNum  Interface   Configuration
 AA3456789012345  1      3          GE1/1         poe enable
                                       GE1/2        poe priority critical
                                       GE1/3

 poe-profileAA    2      1           GE1/24       poe enable
                                                     poe max-power 12300

 poe-profileBB    3      0                         poe enable
                                                     poe priority critical
                                                     poe max-power 15400
                                                     poe mode spare

 ---  3 poe-profile(s) created, 4 port(s) applied  ---
```

Table 646 Description on fields of the display poe-profile command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
poe-profile(s) created	Number of PoE configuration files
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file whose index number is 1.

```
<Sysname> display poe-profile index 1
 Poe-profile      Index  ApplyNum  Interface  Configuration
 AA3456789012345  1      2           GE1/2       poe enable
                                       GE1/24      poe priority critical
                                                    poe max-power 12300
                                                    poe mode spare

 ---  2 port(s) applied  ---
```

Table 647 Description on fields of the display poe-profile index command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

Display all information of the configurations and applications of the PoE configuration file named AA.

```
<Sysname> display poe-profile name AA
 Poe-profile      Index  ApplyNum  Interface  Configuration
 AA                 1       2         GE1/0      poe enable
                                      GE1/1       poe priority critical
                                                   poe max-power 12300
                                                   poe mode spare
---  2 port(s) applied  ---
```

Table 648 Description on fields of the display poe-profile name command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which a PoE configuration file is applied

Table 648 Description on fields of the display poe-profile name command

Field	Description
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Configuration	Configurations of the PoE configuration file
port(s) applied	Sum of the number of PoE interfaces to which all PoE configuration files are respectively applied

display poe-profile interface

Syntax **display poe-profile interface** *interface-type interface-number*

View Any view

Parameter *interface-type interface-number*: Interface type and interface number.

Description Use the **display poe-profile interface** command to display all information of the configurations and applications of the PoE configuration file that currently take effect on the specified PoE interface.

Example # Display all information of the configurations and applications of the current PoE configuration file applied to Ethernet1/0.

```
<Sysname> display poe-profile interface ethernet 1/0
Poe-profile      Index  ApplyNum  Interface  Current Configuration
AA3456789012345  1      2          Eth1/2      poe enable
                                                   poe priority critical
```

Table 649 Description on fields of the display poe-profile interface command

Field	Description
Poe-profile	Name of the PoE configuration file
Index	Index number of the PoE configuration file
ApplyNum	Number of PoE interfaces to which the PoE configuration file is applied
Interface	Shortened form of the PoE interface to which the PoE configuration is applied
Current Configuration	Configurations of the PoE configuration file that currently take effect on a PoE interface

Because not all the configurations of a PoE configuration file are applied successfully, only the configurations that currently take effect on the interface are displayed.

poe disconnect

Syntax **poe disconnect** { **ac** | **dc** }

undo poe disconnect

View System view

Parameter **ac**: Specifies the PD disconnection detection mode as **ac** mode.

dc: Specifies the PD disconnection detection mode as **dc** mode.

Description Use the **poe disconnect** command to configure a PD disconnection detection mode.

Use the **undo poe disconnect** command to restore the default PD disconnection detection mode.

The default PD disconnection detection mode depends on the device model.

Note that a change to the PD disconnection detection mode may lead to a power-off of some PDs.

Example # Set the PD disconnection detection mode to **dc**.

```
<Sysname> system-view
[Sysname] poe disconnect dc
```

poe enable

Syntax **poe enable**

undo poe enable

View PoE interface view/PoE-profile file view

Parameter None

Description Use the **poe enable** command to enable PoE on a PoE interface.

Use the **undo poe enable** command to disable PoE on a PoE interface.

By default, PoE is disabled on a PoE interface.

CAUTION:

- *If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.*
- *If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.*

Example # Enable PoE on a PoE interface.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]poe enable
```

Enable PoE through a PoE configuration file on a PoE interface.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe enable
[Sysname-poe-profile-abc-1] quit
[Sysname] interface ethernet 1/1
[Sysname-Ethernet1/1]apply poe-profile name abc
```

poe enable pse

Syntax **poe enable pse** *pse-id*

undo poe enable pse *pse-id*

View System view

Parameter *pse-id*: PSE ID. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe enable pse** command to enable PoE for the PSE.

Use the **undo poe enable pse** command to disable PoE for the PSE.

By default, PoE is disabled for the PSE.

The support for this command varies with devices.

Example # Enable PoE for PSE 2.

```
<Sysname> system-view
[Sysname] poe enable pse 2
```

poe legacy enable

Syntax **poe legacy enable** [**pse** *pse-id*]

undo poe legacy enable [**pse** *pse-id*]

View System view

Parameter **pse** *pse-id*: Specifies a PSE ID. The support for the argument varies with devices. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe legacy enable** command to enable the PSE to detect nonstandard PDs.

Use the **undo poe legacy enable** command to disable the PSE from detecting nonstandard PDs.

By default, the PSE is disabled from detecting nonstandard PDs.

Example # Enable PSE 2 to detect nonstandard PDs.

```
<Sysname> system-view
[Sysname] poe legacy enable pse 2
```

poe max-power

Syntax **poe max-power** *max-power*

undo poe max-power

View PoE interface view/PoE-profile file view

Parameter *max-power*: Maximum power in milliwatts allocated to a PoE interface. The range of this argument varies with devices.

Description Use the **poe max-power** command to configure the maximum power for a PoE interface.

Use the **undo poe max-power** command to restore the default maximum power of a PoE interface.

By default, the maximum power of the PoE interface is 15,400 milliwatts.

Example # Set the maximum power of Ethernet 1/0 to 12,000 milliwatts.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] poe max-power 12000
```

Set the maximum power of Ethernet 1/0 to 12,000 milliwatts through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe max-power 12000
[Sysname-poe-profile-abc-1] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]apply poe-profile name abc
```

poe max-power (system view)

Syntax **poe max-power** *max-power* [**pse** *pse-id*]

undo poe max-power [**pse** *pse-id*]

View System view

Parameter *max-power*: Maximum power in watts of the PSE. The support for the value varies with devices.

pse *pse-id*: Specifies a PSE ID. The support for this argument varies with devices. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe max-power** command to configure the maximum power for the PSE.

Use the **undo poe max-power** command to restore the default maximum power of the PSE.

The default maximum power of the PSE varies with devices.

Note that:

- The maximum power of the PSE must be greater than or equal to the sum of the maximum power of all critical PoE interfaces on the PSE so as to guarantee the power supply to these PoE interfaces. When the consumption power of all PDs connected to the PSE is greater than the maximum power of the PSE, some PDs will be powered off.
- The sum of the maximum power of all PSEs must be less than the maximum PoE power.

Related command: **poe priority (system view)**.

Example # Set the maximum power of PSE 2 to 150 watts.

```
<Sysname> system-view
[Sysname] poe max-power 150 pse 2
```

poe mode

Syntax **poe mode** { **signal** | **spare** }

undo poe mode

View PoE interface view/PoE-profile file view

Parameter **signal**: Specifies the PoE mode as **signal** (power over signal cables).

spare: Specifies the PoE mode as **spare** (power over spare cables).

Description Use the **poe mode** command to configure a PoE mode.

Use the **undo poe mode** command to restore the default PoE mode.

By default, the PoE mode is **signal** (power over signal cables).

The PSE supplies power for a PoE interface in the following two modes: **signal** and **spare**.

- In the signal mode, lines in Category 3 and 5 twisted pair cables used for transmitting data are also used for supplying DC power.
- In the spare mode, lines in Category 3 and 5 twisted pair cables not in use are used for supplying DC power.

Example # Set the PoE mode to **signal** (power over signal cables).

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]poe mode signal
```

Set the PoE mode to **signal** (power over signal cables) through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe mode signal
[Sysname-poe-profile-abc-1] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]apply poe-profile name abc
```

poe pd-description

Syntax **poe pd-description** *string*

undo poe pd-description

View PoE interface view

Parameter *string*: Description of the PD connected to a PoE interface, up to 80 characters.

Description Use the **poe pd-description** command to configure a description for the PD connected to a PoE interface.

Use the **undo poe pd-description** command to restore the default.

By default, no description is available for the PD connected to a PoE interface.

Example # Describe the PD connected to Ethernet1/0 as IP Phone For Room 101.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]poe pd-description IP Phone For Room 101
```

poe pd-policy priority

Syntax **poe pd-policy priority**

undo poe pd-policy priority

View System view

Parameter None

Description Use the **poe pd-policy priority** command to configure a PD power management priority policy.

Use the **undo poe pd-policy priority** command to remove the PD power management priority policy.

By default, no PD power management priority policy is configured.

Example # Configure a PD power management priority policy

```
<Sysname> system-view
[Sysname] poe pd-policy priority
```

poe priority

Syntax **poe priority** { **critical** | **high** | **low** }

undo poe priority

View PoE interface view/PoE-profile file view

Parameter **critical**: Sets the power priority of a PoE interface to **critical**. The PoE interface whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PD connected to this critical PoE interface.

high: Sets the power priority of a PoE interface to **high**.

low: Sets the power priority of a PoE interface to **low**.

Description Use the **poe priority** command to configure a power priority level for a PoE interface.

Use the **undo poe priority** command to restore the default power priority level.

By default, the power priority of a PoE interface is **low**.

Note that:

- When the PoE power is insufficient, power is first supplied to PoE interfaces with a higher priority level.
- If a PoE configuration file is already applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE-profile view.
- If a PoE configuration file is applied to a PoE interface, you need to remove the application of the file to the PoE interface before configuring the interface in PoE interface view.

- If two PoE interfaces have the same priority level, the PoE interface with a smaller ID has the higher priority level. The support for the PoE interface priority level varies with devices.

Example # Set the power priority of Ethernet 1/0 to **critical**.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] poe priority critical
```

Set the power priority of Ethernet 1/0 to **critical** through a PoE configuration file.

```
<Sysname> system-view
[Sysname] poe-profile abc
[Sysname-poe-profile-abc-1] poe priority critical
[Sysname-poe-profile-abc-1] quit
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0]apply poe-profile name abc
```

poe priority (system view)

Syntax **poe priority** { **critical** | **high** | **low** } [**pse** *pse-id*]

undo poe priority [**pse** *pse-id*]

View System view

Parameter **critical**: Sets the power priority level of the PSE to **critical**. The PSE whose power priority level is **critical** works in guaranteed mode, that is, power is first supplied to the PSE.

high: Sets the power priority of the PSE to **high**.

low: Sets the power priority of the PSE to **low**.

pse *pse-id*: Specifies a PSE ID. The support for this argument varies with devices. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe priority** command to configure a power priority level for the PSE.

Use the **undo poe priority** command to restore the default power priority level of the PSE.

By default, the power priority level of the PSE is **low**.

When the PoE power is insufficient, power is first supplied to PSE with a higher power priority level.

Example # Set the power priority of PSE 2 to **critical**.

```
<Sysname> system-view
[Sysname] poe priority critical pse 2
```

poe pse-policy priority

Syntax **poe pse-policy priority**

undo poe pse-policy priority

View System view

Parameter None

Description Use the **poe pse-policy priority** command to configure a PSE power management priority policy.

Use the **undo poe pse-policy priority** command to remove the PSE power management priority policy.

By default, no PSE power management priority policy is configured.

Example # Configure a PSE power management priority policy.

```
<Sysname> system-view
[Sysname] poe pse-policy priority
```

poe update

Syntax **poe update** { **full** | **refresh** } *filename* [**pse** *pse-id*]

View System view

Parameter **full**: Specifies to upgrade the PSE processing software in full mode when the software is unavailable.

refresh: Specifies to upgrade the PSE processing software in refresh mode when the software is available.

filename: Name of the upgrade file, a string of 1 to 64 characters. This file must be under the root directory of the file system of the device. The extension of the upgrade file varies with devices.

pse *pse-id*: Specifies a PSE ID. The support for this argument varies with devices. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe update** command to upgrade the PSE processing software online.

Example # Upgrade the processing software of PSE 2 online

```
<Sysname> system-view
[Sysname] poe update refresh 0400_001.S19 pse 2
```

poe utilization-threshold

Syntax **poe utilization-threshold** *utilization-threshold-value* [**pse** *pse-id*]

undo poe utilization-threshold [**pse** *pse-id*]

View System view

Parameter *utilization-threshold-value*: Power alarm threshold in percentage, in the range 1 to 99.

pse *pse-id*: Specifies a PSE ID. The support for this argument varies with devices. *pse-id* indicates number of the slot where a PoE interface locates.

Description Use the **poe utilization-threshold** command to configure a power alarm threshold for the PSE.

Use the **undo poe utilization-threshold** command to restore the default power alarm threshold of the PSE.

By default, the power alarm threshold for the PSE is 80%.

The system sends a Trap message when the percentage of power utilization exceeds the alarm threshold. If the percentage of the power utilization always keeps above the alarm threshold, the system does not send any Trap message. Instead, when the percentage of the power utilization drops below the alarm threshold, the system sends a Trap message again.

Example # Set the power alarm threshold of PSE 2 to 90%.

```
<Sysname> system-view
[Sysname] poe utilization-threshold 90 pse 2
```

poe-profile

Syntax **poe-profile** *profile-name* [*index*]

undo poe-profile { **index** *index* | **name** *profile-name* }

View System view

Parameter *profile-name*: Name of a PoE configuration file, a string of 1 to 15 characters. A PoE configuration file name begins with a letter (a through z or A through Z) and must not contain reserved keywords such as **undo**, **all**, **name**, **interface**, **user**, **poe**, **disable**, **max-power**, **mode**, **priority** and **enable**.

index: Index number of a PoE configuration file, in the range of 1 to 100.

Description Use the **poe-profile** *profile-name* command to create a PoE configuration file and enter PoE-profile view.

Use the **undo poe-profile** command to delete the specified PoE configuration file.

If no index is specified, the system will automatically assign an index to the PoE configuration file, starting from 1.

If a PoE configuration file is already applied to a PoE interface, you cannot delete it. To delete the file, you must first execute the **undo apply poe-profile** command to remove the application of the PoE configuration file to the PoE interface.

Example # Create a PoE configuration file, name it abc, and specify the index number as 3.

```
<Sysname> system-view
[Sysname] poe-profile abc 3
```

167 OAP MODULE CONFIGURATION COMMANDS

NOTE: *In some regions, the OAP modules are sold as "OSM" modules. They are identical in function.*

oap connect slot

Syntax **oap connect slot** *slot-number*

View User view

Parameter *slot-number:* Number of the slot where an OAP module locates.

Description Use the **oap connect slot** command to switch from the command line interface on the router to the Linux OS on an OAP module.

You can press <Ctrl+k> to return from the Linux OS on an OAP module to the command line interface on the router.

Example # Switch from command line interface on the router to the OS on an OAP module.

```
<Sysname> oap connect slot 3
Connected to OAP
```

Press <Enter> to log onto the Linux OS after the above prompt appears.

```
Red Hat Linux release 9 (Shrike)
Kernel 2.4.20-8custom on an i686

OAP login: root
Password:
Last login: Mon Jul  3 16:48:56 on ttyS0
You have new mail.
[root@OAP root]#
```

Press <Ctrl+k> to return to the command line interface on the router.

```
<Sysname>
```

oap reboot slot

Syntax **oap reboot slot** *slot-number*

View User view

Parameter *slot-number:* Number of the slot where an OAP module locates.

Description Use the **oap reboot slot** command to restart an OAP module, which equals to resetting the OAP module by pressing the Reset button on the OAP module.

CAUTION: *Before resetting an OAP module you are recommended to save the data on Linux OS and shut down the Linux OS to avoid service interruption and hardware data loss. After the reset, the Linux OS on the OAP module will be automatically rebooted.*

Related command: oap reload slot, oap shutdown slot.

Example # Restart the OAP module on slot 3.

```
<Sysname> oap reboot slot 3
This command will recover the OAP from shutdown or other failed state.
Warning: This command may lose the data on the hard disk if the OAP is not b
eing shut down!
Continue? [Y/N] y
Reboot OAP by command.
```

168 ACFP CONFIGURATION COMMANDS

acfp enable

Syntax **acfp enable**

undo acfp enable

View System view

Parameters None

Description Use the **acfp enable** command to enable ACFP.

Use the **undo acfp enable** command to disable ACFP.

ACFP is disabled by default.

Example # Enable ACFP.

```
<Sysname> system-view
[Sysname] acfp enable
```

display acfp client-info

Syntax **display acfp client-info** [*client-id*]

View Any view

Parameters *client-id*: Displays information of the specified ACFP client, where *client-id* represents the ACFP client ID, in the range of 1 to 2147483647.

Description Use the **display acfp client-info** command to display the information about the specified ACFP client(s).

Note that:

- If ACFP client ID is specified, the information about the specified ACFP client is displayed.
- If no ACFP client ID is specified, the information about all the ACFP clients is displayed.

Example # Display the information about all the ACFP clients.

```
<Sysname> display acfp client-info
ACFP client total number: 1
ClientID:     4
Description:  IPS
Hw-Info:      1.0
OS-Info:      Linux Kernel 2.4.20-8
App-Info:     2.0
Client IP:    10.1.1.1
Client Mode:  mirror
```

Table 650 Description on the fields of the display acfp client-info command

Field	Description
ACFP client total number	Total number of ACFP clients
ClientID	Client ID, index of client list
Description	Description information of client application program
Hw-Info	Hardware information of the client
OS-Info	Operating system information of the client
App-Info	Application software information of the client
Client IP	Client IP address
Client Mode	Working modes supported by the client: ■ Ipserver: host mode ■ Redirect: redirect mode ■ Mirror: mirror mode ■ Passthrough: pass-through mode

display acfp policy-info

Syntax **display acfp policy-info** [**client** *client-id* [*policy-index*] | **dest-interface** *interface-type interface-number* | **in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] [**active** | **inactive**]

View Any view

Parameters **client** *client-id*: Displays the policy applied sent by the specified ACFP client, where *client-id* is the ACFP client ID, in the range of 1 to 2147483647.

policy-index: Policy index, in the range of 1 to 2147483647.

dest-interface *interface-type interface-number*: Displays all the policies that use the specified interface (destination interface) for connecting to the ACFP client, where *interface-type interface-number* is the interface type and interface number.

in-interface *interface-type interface-number*: Displays all the policies that use the specified interface as the inbound interface, where *interface-type interface-number* is the interface type and interface number.

out-interface *interface-type interface-number*: Displays all the policies that use the specified interface as the outbound interface, where *interface-type interface-number* is the interface type and interface number.

active: Displays active policies only.

inactive: Displays inactive policies only.

Description

Use the **display acfp policy-info** command to display the ACFP policy information.

Note the following:

- When you use this command to display the policy information applied by the specified ACFP client, if you specify the *policy-index* argument, the command will display the information about the policy whose number is *policy-index* delivered by the ACFP client with an ID of *client-id*. Otherwise, the command will display the information about all the policies delivered by the ACFP client with an ID of *client-id.*
- If neither the **active** nor **inactive** keyword is specified, the command will display all the active or inactive policies.
- If no argument is specified, the command will display the information about all the policies.

Example

Display the information about the effective policies for all the interfaces that use Ethernet 1/0 as the inbound interface.

```
<Sysname> display acfp policy-info in-interface ethernet 1/0 active
ACFP policy total number: 1
ClientID:        1                   Policy-Index:    2
Rule-Num:        20                  ContextID:       2007
Exist-Time:      100000(s)           Life-Time:       864000(s)
Start-Time:      9:00                End-Time:        12:00
Admin-Status:    enable              Effect-Status:   active
In-Interface:    e1/0
Out-Interface:   e1/1
Dest-Interface:  g0/0
```

Table 651 Description on the fields of the display acfp policy-info command

Field	Description
ACFP policy total number	Total number of ACFP policies
ClientID	Client ID, index of the client list
Policy-Index	Policy index
Rule-Num	Number of rules under the policy
ContextID	Context ID of the packet
Exist-Time	For how long the policy has existed, in seconds
Life-Time	Policy validity, in seconds
Start-Time	Policy start time
End-Time	Policy end time
Admin-Status	Policy administration status
Effect-Status	Whether the policy effective

Table 651 Description on the fields of the display acfp policy-info command

Field	Description
In-Interface	Inbound interface of the packet
Out-Interface	Outbound interface of the packet
Dest-Interface	Interface connected to the ACFP client

display acfp rule-cache

Syntax **display acfp rule-cache** [**in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] *

View Any view

Parameters **in-interface** *interface-type interface-number*: Displays the rule cache information of the specified inbound interface, where *interface-type interface-number* is the interface type and interface number.

out-interface *interface-type interface-number*: Displays the rule cache information of the specified outbound interface, where *interface-type interface-number* is the interface type and interface number.

Description Use the **display acfp rule-cache** command to display ACFP rule cache information.

If you specify neither the **in-interface** nor **out-interface** keyword, the command will display all the ACFP rule cache information.

Example # Display all the ACFP rule cache information.

```
<Sysname> display acfp rule-cache
ACFP rule-cache total items: 2


Idx  SIP             Sport DIP             DPort Pro  InIf    OutIf
-------------------------------------------------------------------------
1021 202.153.124.111 62534 202.124.152.234 32456 4    g0/2    e1/1

Precedence    ToS   DSCP   Establish   Fragment   Action
-----------------------------------------------------------
7             15    Af12   false       true       redirect


Idx  SIP             Sport DIP             DPort Pro  InIf   OutIf
-------------------------------------------------------------------------
895  202.153.124.111 62534 202.124.152.234 32456 1    g0/2   e1/1

Precedence    ToS   DSCP   Establish   Fragment   Action
-----------------------------------------------------------
3             14    Be     false       true       deny
```

Table 652 Description on the fields of the display acfp rule-cache command

Field	Description
ACFP rule-cache total items	Number of ACFP rule cache information entries

Table 652 Description on the fields of the display acfp rule-cache command

Field	Description
Idx	Hash index
SIP	Source IP address
SPort	Source port number
DIP	Destination IP address
DPort	Destination port number
Pro	Protocol of the packet, in the range of 0 to 255
InIf	Inbound interface of the packet
OutIf	Outbound interface of the packet
Precedence	Packet precedence, a number in the range of 0 to 7
Tos	Type of service, a number in the range of 0 to 15
DSCP	Differentiated services codepoint, containing 0 to 63 characters for Be, Ef, Af11, Af12, Af13, Af21, Af22, Af23, Af31, Af32, Af33, Af41, Af42, Af43, Cs1, Cs2, Cs3, Cs4, Cs5, Cs6, and Cs7 and 0 to 63 numbers for other modes
Establish	Whether the packet is a TCP connection establishing packet: true (TCP connection establishing packet) and false (non-TCP connection establishing packet)
Fragment	Whether the packet is a fragment: true (fragment) and false (non-fragment)
Action	Action: permit, deny, mirror, and redirect

display acfp rule-info

Syntax **display acfp rule-info** { **in-interface** [*interface-type interface-number*] | **out-interface** [*interface-type interface-number*] | **policy** [*client-id policy-index*] }

View Any view

Parameters **in-interface**: Displays ACFP rule information in order of inbound interface. The ACFP rule information which does not include the inbound interface is not displayed.

out-interface: Displays ACFP rule information in order of outbound interface. The ACFP rule information which does not include the outbound interface is not displayed.

interface-type interface-number: Specifies an interface by interface type and interface number.

policy: Displays the ACFP rule information in order of policy.

client-id: ACFP client ID, in the range of 1 to 2147483647.

policy-index: Policy index, in the range of 1 to 2147483647.

Description Use the **display acfp rule-info** command to display ACFP rule information.

Note the following:

- When you use this command to display ACFP rule information in order of policy, if you specify neither client ID nor policy index, the rule information of all the policies will be displayed.
- When you use this command to display ACFP rule information in order of outbound/inbound interface, if you specify no interface, the rule information for all the inbound interfaces or outbound interfaces will be displayed.

Example # Display ACFP rule information in order of inbound interface.

```
<Sysname> display acfp rule-info in-interface ethernet 1/0
In-Interface:           e1/0
ACFP rule total number: 1
ClientID:2              Policy-Index:2          Rule-Index:5
SIP:192.168.132.123     SMask:0.0.0.255         SPort:65500 to 65535
DIP:192.168.112.114     DMask:0.0.0.255         DPort:65500 to 65535
Protocol:ipinip         Establish:false   Fragment:false   Tos:1     Pre:1
Action:redirect         Status:active
```

Display ACFP rule information in order of policy.

```
<Sysname> display acfp rule-info policy 1 1
ACFP Rule total number: 1
ClientID:1              Policy-Index:1          Rule-Index:1
SIP:192.168.132.122     SMask:0.0.0.255         SPort:65500 to 65535
DIP:192.168.112.115     DMask:0.0.0.255         DPort:65500 to 65535
Protocol:ipinip         Establish:false   Fragment:false   DSCP:AF11
Action:redirect         Status:inactive
```

Table 653 Description on the fields of the display acfp rule-info command

Field	Description
In-Interface	Inbound interface of the packet
Out-Interface	Outbound interface of the packet
ACFP rule total number	Total number of ACFP rules
ClientID	Client ID, index of client list
Policy-Index	Policy index
Rule-Index	Rule index
ContextID	Context ID
SIP	Source IP address
SMask	Inverse mask of source IP address
SPort	Source port number
DIP	Destination IP address
DMask	Inverse mask of destination IP address
DPort	Destination port number
Protocol	Protocol of the packet: GRE, ICMP, IGMP, IPinIP, OSPF, TCP, UDP, IP, and so on.
Establish	Whether the packet is a TCP connection establishing packet: true (TCP connection establishing packet) and false (indicates all the packets, not concerned about whether the packet is a TCP connection establishing packet)
Fragment	Whether the packet is a fragment: true (fragment) and false (indicates all the packets, not concerned about whether the packet is a fragment)

Table 653 Description on the fields of the display acfp rule-info command

Field	Description
Tos	Type of service, a number in the range of 0 to 15
Pre	Packet precedence, a number in the range of 0 to 7
DSCP	Differentiated services codepoint, containing 0 to 63 characters for Be, Ef, Af11, Af12, Af13, Af21, Af22, Af23, Af31, Af32, Af33, Af41, Af42, Af43, Cs1, Cs2, Cs3, Cs4, Cs5, Cs6, Cs7 and 0 to 63 numbers for other modes
Action	Action: permit, deny, mirror, and redirect
Status	Rule status: active and inactive

display acfp server-info

Syntax **display acfp server-info**

View Any view

Parameters None

Description Use the **display acfp server-info** command to display ACFP server information.

Example # Display ACFP server information.

```
<Sysname> display acfp server-info
Server-Info:     ipserver redirect mirror
Max Life-Time:   2147483647(s)
PersistentRules: false
ContextType:     router-context
```

Table 654 Description on the fields of the display acfp server-info command

Field	Description
Server-Info	Client working modes supported by the server: ■ Ipserver: host mode ■ Redirect: redirect mode ■ Mirror: mirror mode ■ Passthrough: pass-through mode
Max Life-Time	Maximum validity, in seconds, of the cooperation policy supported by the server
PersistentRules	Whether the server supports persistent cooperation rules
ContextType	Context ID types currently supported by the server: ■ no-context: No context ID is carried. ■ router-context: The packet carrying the context ID is suitable for a router. ■ switch-context: The packet carrying the context ID is suitable for a switch.

reset acfp rule-cache

Syntax **reset acfp rule-cache** [**in-interface** *interface-type interface-number* | **out-interface** *interface-type interface-number*] *

View User view

Parameters **in-interface** *interface-type interface-number*: Clears the ACFP rule cache for the specified inbound interface, where *interface-type interface-number* is the interface type and interface number.

out-interface *interface-type interface-number*: Clears the ACFP rule cache for the specified outbound interface, where *interface-type interface-number* is the interface type and interface number.

Description Use the **reset acfp rule-cache** command to clear ACFP rule cache.

If you specify no inbound interface or outbound interface, the ACFP rule cache on all the inbound interfaces or outbound interfaces will be cleared.

Example # Clear the ACFP rule cache that uses Ethernet 1/1.as the inbound interface.

```
<Sysname> reset acfp rule-cache in-interface ethernet 1/1
```

169 ACSEI SERVER CONFIGURATION COMMANDS

acsei server enable

Syntax **acsei server enable**

undo acsei server enable

View System view

Parameters None

Description Use the **acsei server enable** command to enable ACSEI server.

Use the **undo acsei server enable** command to disable ACSEI server.

By default, ACSEI server is disabled.

Examples # Enable ACSEI server.

```
<Sysname> system-view
[Sysname] acsei server enable
```

acsei server

Syntax **acsei server**

View System view

Parameters None

Description Use the **acsei server** command to enter ACSEI server view.

Examples # Enter ACSEI server view.

```
<Sysname> system-view
[Sysname] acsei server
[Sysname-acsei-server]
```

acsei timer clock-sync

Syntax **acsei timer clock-sync** *minutes*

undo acsei timer clock-sync

View ACSEI server view

Parameters *minutes*: Value of the synchronization timer that is used for clock synchronization from ACSEI server to ACSEI client. It ranges from 0 to 1440 (in minutes), where value 0 specifies to inhibit the clock synchronization from ACSEI server to ACSEI client.

Description Use the **acsei timer clock-sync** command to set the synchronization timer that is used for clock synchronization from ACSEI server to ACSEI client.

Use the **undo acsei timer clock-sync** command to restore the default value for the synchronization timer.

By default, the sychronization timer is set to five minutes.

Examples # Set the synchronization timer from ACSEI server to ACSEI client to 20 minutes.

```
<Sysname> system-view
[Sysname] acsei server
[Sysname-acsei-server] acsei timer clock-sync 20
```

acsei timer monitor

Syntax **acsei timer monitor** *seconds*

undo acsei timer monitor

View ACSEI server view

Parameters *seconds*: Value of the monitor timer that is used for ACSEI server to monitor ACSEI clients. It ranges from 0 to 10 (in seconds), where 0 specifies to disable ACSEI server from monitoring ACSEI client.

Description Use the **acsei timer monitor** command to set the monitor timer for ACSEI server to monitor ACSEI client.

Use the **undo acsei timer monitor** command to restore the default value for the monitor timer.

By default, the monitor timer is set to five seconds.

Examples # Set the monitor timer for ACSEI server to monitor ACSEI client to six seconds.

```
<Sysname> system-view
[Sysname] acsei server
[Sysname-acsei-server] acsei timer monitor 6
```

acsei client close

Syntax **acsei client close** *client-id*

View ACSEI server view

Parameters *client-id*: ID of the ACSEI client to be closed, in the range of 1 to 10. (An ACSEI client ID is assigned by the ACSEI server.)

Description Use the **acsei client close** command to close a specified ACSEI client.

Examples # Close the ACSEI client with ID of 1.

```
<Sysname> system-view
[Sysname] acsei server
[Sysname-acsei-server] acsei client close 1
```

acsei client reboot

Syntax **acsei client reboot** *client-id*

View ACSEI server view

Parameters *client-id*: ID of the ACSEI client to be restarted, in the range of 1 to 10.

Description Use the **acsei client reboot** command to restart ACSEI client.

Examples # Restart the ACSEI client with ID of 1.

```
<Sysname> system-view
[Sysname] acsei server
[Sysname-acsei-server] acsei client reboot 1
```

display acsei client summary

Syntax **display acsei client summary** [*client-id*]

View Any view

Parameters *client-id*: ID of an ACSEI client, in the range 1 to 10.

Description Use the **display acsei client summary** command to display ACSEI client summary information, including the status of the ACSEI client, the interface

carrying the ACSEI client, and the last registration time of the ACSEI client. Summary information of multiple ACSEI clients is displayed in order of registration time.

If executed without the *client-id* argument, the command displays summary information about all the ACSEI clients.

Examples # Display the summary of ACSEI client 1.

```
<Sysname>display acsei client summary 1
client ID: 1
Status: Open
MAC Address: 00e0-fc0a-c3ef
Interface: GigabitEthernet5/0
Last registered: 02/08/2007 12:00:00
```

Display the summary of all ACSEI clients.

```
<Sysname> display acsei client summary
Total client Number: 2

client ID: 1
Status: Open
MAC Address: 00e0-fc0a-c3ef
Interface: GigabitEthernet5/0
Last registered: 02/08/2007 12:00:00

client ID: 2
Status: Open
MAC Address: 00e0-fa1e-03da
Interface: GigabitEthernet6/0
Last registered: 02/08/2007 13:00:00
```

Table 655 Description on the fields of the display acsei client summary command

Field	Description
client ID	ID of the ACSEI client
Status	ACSEI client status
MAC Address	MAC address of the ACSEI client
Interface	Interface carrying the ACSEI client
Last registered	The last registration time of the ACSEI client

display acsei client info

Syntax **display acsei client info** [*client-id*]

View Any view

Parameters *client-id*: ID of an ACSEI client, in the range 1 to 10.

Description Use the **display acsei client info** command to display the ACSEI client information. The information is retrieved from the advertisement packet sent by

the client, so that when there's no ACSEI client information, the command displays the information keywords only.

If executed without the *client-id* argument, the command displays information about all the ACSEI clients in order of registration time.

Examples # Display information about ACSEI client 5.

```
<Sysname>display acsei client info 1
 client ID: 1
 client Description:
 Hardware:
 System Software:
 Application Software:
 CPU: Intel(R) Pentium(R) M processor 1.40GHz
 PCB Version: 3.00
 CPLD Version: 1.00
 Bootrom Version: 1.12
 CF card: 256 MB
 Memory: 512 MB
 Harddisk: 40.0 GB
```

Display information about all ACSEI clients.

```
<Sysname> display acsei client info
Total client Number: 2

client ID: 1
client Description:
 Hardware:
 System Software:
 Application Software:
 CPU: Intel(R) Pentium(R) M processor 1.40GHz
 PCB Version: 3.00
 CPLD Version: 1.00
 Bootrom Version: 1.12
 CF card: 256 MB
 Memory: 512 MB
Harddisk: 40.0 GB

client ID: 2
client Description:
Hardware:
System Software:
Application Software:
CPU: Intel(R) Pentium(R) M processor 1.40GHz
PCB Version: 3.00
CPLD Version: 1.00
Bootrom Version: 1.12
CF card: 256 MB
Memory: 512 MB
Harddisk: 40.0 GB
```

Table 656 Description on the fields of the display acsei client info command

Field	Description
client ID	ID of the ACSEI client

Table 656 Description on the fields of the display acsei client info command

Field	Description
client Description	ACSEI client description
Hardware	Hardware version of the ACSEI client
System Software	System software name and version of the ACSEI client
Application Software	Application name and version of the ACSEI client
CPU	CPU information of the ACSEI client
PCB Version	PCB version of the ACSEI client
CPLD Version	CPLD version of the ACSEI client
Bootrom Version	Boot ROM version of the ACSEI client
CF card	CF card information of the ACSEI client
Memory	Memory information of the ACSEI client
Harddisk	Harddisk information of the ACSEI client

170 ACSEI CLIENT CONFIGURATION COMMANDS

- *Multiple kinds of ACSEI clients have been developed at present. Different ACSEI clients need different configuration. The following commands are available for the ACSEI client running on an OAP module.*
- *The following commands can be executed in any directory of the Linux system. You can use the **oap connect slot** command in user view of the device to enter the Linux system of the OAP module. For description on the **oap connect slot** command, refer to "oap connect slot" on page 2507.*

acsei-client debug disable

Syntax **acsei-client debug disable**

View Any directory of the Linux system

Parameters None

Description Use the **acsei-client debug disable** command to disable debugging for ACSEI client.

By default, debugging for ACSEI client is disabled.

Examples # The OAP module locates in slot 6. Disable debugging for ACSEI client.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# acsei-client debug disable
```

acsei-client debug enable

Syntax **acsei-client debug enable**

View Any directory of the Linux system

Parameters None

Description Use the **acsei-client debug enable** command to enable debugging for ACSEI client.

By default, debugging for ACSEI client is disabled.

Examples # Enable debugging for ACSEI client.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# acsei-client debug enable
```

acsei-client debug show

Syntax **acsei-client debug show**

View Any directory of the Linux system

Parameters None

Description Use the **acsei-client debug show** command to display the debugging information about ACSEI client.

By default, no ACSEI client debugging will be displayed.

ACSEI client debugging is displayed through a pipe; therefore, part of the debugging information may fail to be displayed when the pipe is full.

Examples # Display the ACSEI client debugging information.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# acsei-client debug enable
[root@localhost ~]# acsei-client debug show
```

chkconfig acseid off

Syntax **chkconfig acseid off**

View Any directory of the Linux system

Parameters None

Description Use the **chkconfig acseid off** command to configure not to start up ACSEI client automatically, that is, configure not to start up ACSEI client simultaneously with the system.

By default, ACSEI client installed on the OAP module is started up automatically when the system is started up.

Examples # Configure not to start up ACSEI client automatically when the system is started up.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# chkconfig acseid off
```

chkconfig acseid on

Syntax **chkconfig acseid on**

View Any directory of the Linux system

Parameters None

Description Use the **chkconfig acseid on** command to configure to start up ACSEI client automatically, that is, configure to start up ACSEI client simultaneously with the system.

By default, ACSEI client installed on the OAP module is started up automatically when the system is started up.

Examples # Configure to start up ACSEI client automatically when the system is started up.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# chkconfig acseid on
```

service acseid condrestart

Syntax **service acseid condrestart**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid condrestart** command to restart ACSEI client conditionally. That is, if ACSEI client is running, this command stops the process before it restarts the process; if ACSEI client is not running, this command does not restart the process.

Examples # Execute conditional restart of ACSEI client (when ACSEI client is running).

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon (pid 2849) is running...
[root@localhost ~]# service acseid condrestart
Stopping acseic-daemon: [  OK  ]
Starting acseic-daemon: [  OK  ]
```

Execute conditional restart of ACSEI client (when ACSEI client is stopped).

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon is stopped
[root@localhost ~]# service acseid condrestart
[root@localhost ~]#
```

service acseid reload

Syntax **service acseid reload**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid reload** command to load the ACSEI client configuration file.

You can load the ACSEI client configuration file only when the ACSEI client is started. Otherwise, you will fail to load the ACSEI client configuration file.

Examples # Load the ACSEI client configuration file.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon (pid 2849) is running...
[root@localhost ~]# service acseid reload
Reloading configuration: [  OK  ]
```

service acseid restart

Syntax **service acseid restart**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid restart** command to restart an ACSEI client.

Examples # Restart a running ACSEI client.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon (pid 2849) is running...
[root@localhost ~]# service acseid restart
```

```
Stopping acseic-daemon: [  OK  ]
Starting acseic-daemon: [  OK  ]
```

Restart a stopped ACSEI client.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon is stopped
[root@localhost ~]# service acseid restart
Stopping acseic-daemon: [FAILED]
Starting acseic-daemon: [  OK  ]
```

service acseid start

Syntax **service acseid start**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid start** command to start an ACSEI client.

By default, the ACSEI client installed on the OAP module is started.

Examples # Start an ACSEI client that is running.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid start
Starting acseic-daemon:
```

Start an ACSEI client that is stopped.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid start
Starting acseic-daemon: [  OK  ]
```

service acseid status

Syntax **service acseid status**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid status** command to query the running status of an ACSEI client.

Examples # Query the running status of an ACSEI client that is running.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon (pid 2849) is running...
```

Query the running status of an ACSEI client that is stopped.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon is stopped
```

service acseid stop

Syntax **service acseid stop**

View Any directory of the Linux system

Parameters None

Description Use the **service acseid stop** command to stop an ACSEI client.

By default, the ACSEI client installed on the OAP is started.

Examples # Stop an ACSEI client that is running.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon (pid 2849) is running...
[root@localhost ~]# service acseid stop
Stopping acseic-daemon: [  OK  ]
```

Stop an ACSEI client that is stopped.

```
<Sysname> oap connect slot 6
Connected to OAP!
[root@localhost ~]# service acseid status
acseic-daemon is stopped
[root@localhost ~]# service acseid stop
Stopping acseic-daemon: [FAILED]
```

171 TRACK CONFIGURATION COMMANDS

display track

Syntax **display track** { *track-entry-number* | **all** }

View Any view

Parameters *track-entry-number*: Displays information about the specified Track object, in the range 1 to 1024.

all: Displays information about all the Track objects.

Description Use the **display track** command to display Track object information.

Examples # Display information about all the Track objects.

```
<Sysname> display track all
Track ID: 1
  Status: Positive
  Reference Object:
    NQA Entry: admin test
    Reaction: 10
```

Table 657 Description on the fields of the display track command

Field	Description
Track ID	ID of a Track object
Status	Status of a Track object: ■ Positive: The Track object is normal. ■ Invalid: The Track object is invalid. ■ Negative: The Track object is abnormal.
Reference Object	The objects referenced by the Track object
NQA Entry	The NQA test group referenced by the Track object
Reaction	The Reaction entry referenced by the Track object

track

Syntax **track** *track-entry-number* **nqa entry** *admin-name operation-tag* **reaction** *item-num*

undo track *track-entry-number*

View System view

Parameters *track-entry-number*: Track object ID, in the range 1 to 1024.

admin-name: Name of the administrator creating the NQA operation, a string of 1 to 32 characters, case-insensitive.

operation-tag: NQA operation tag, a string of 1 to 32 characters, case-insensitive.

item-num: Reaction entry ID, in the range 1 to 10.

Description Use the **track** command to create the Track object associated with the specified Reaction entry of the NQA test group.

Use the **undo track** command to delete the created Track object.

By default, no Track object is created.

Note that after a Track object is created, you cannot modify it using the **track** command.

Related commands: **nqa schedule admin-name operation-tag start-time now lifetime forever** on page 2275, reaction in *NQA Commands* in the *System Volume*.

Examples # Create Track object 1 to associate it with Reaction 3 of the NQA test group (admin-test).

```
<Sysname> system-view
[Sysname] track 1 nqa entry admin test reaction 3
```

172 IPX CONFIGURATION COMMANDS

display ipx interface

Syntax **display ipx interface** [*interface-type interface-number*]

View Any view

Parameter *interface-type interface-number*: Displays the IPX information of an interface.

Description Use the **display ipx interface** command to display IPX information on a specified interface.

If no interface is specified, information about all IPX interfaces will be displayed.

Example # Display IPX information on the interface Ethernet 1/1.

```
<Sysname> display ipx interface ethernet 1/1
Ethernet1/1 is up
   IPX address is 1.0000-5e19-1d01 [up]
   SAP is enabled
   Split horizon is enabled
   Update change only is disabled
   Forwarding of IPX type 20 propagation packet is disabled
   Delay of this IPX interface, in ticks is 1
   SAP GNS response is enabled
   RIP packet maximum size is 432 bytes
   SAP packet maximum size is 480 bytes
   IPX encapsulation is Netware 802.3
   0 received, 2 sent
   0 bytes received, 74 bytes sent
   0 RIP received, 1 RIP sent, 0 RIP discarded
   0 RIP specific requests received, 0 RIP specific responses sent
   0 RIP general requests received, 0 RIP general responses sent
   0 SAP received, 0 SAP sent, 0 SAP discarded
   0 SAP requests received, 0 SAP responses sent
```

Table 658 Description on the fields of the display ipx interface command

Field	Description
Ethernet1/1 is up	Ethernet1/1 is up
IPX address	The IPX network number and node number of the current interface
[down] / [up]	IPX protocol status
SAP is enabled	SAP is enabled
Split horizon is enabled	Split horizon is enabled

Table 658 Description on the fields of the display ipx interface command

Field	Description
Update change only is disabled	The triggered update feature is disabled.
Forwarding of IPX type 20 propagation packet is disabled	Forwarding of IPX type 20 propagation packet is disabled.
Delay of this IPX interface	Delay value of the current interface in ticks (a tick is 1/18 second).
SAP GNS response is enabled/disabled	Whether the interface is enabled to respond to SAP GNS requests.
RIP packet maximum size	Maximum size of RIP updating packet on the current interface.
SAP packet maximum size	Maximum size of SAP updating packet on the current interface.
0 received	IPX packets received on the interface
2 sent	IPX packets sent on the interface
0 bytes received	IPX packet bytes received on the interface
74 bytes sent	IPX packet bytes sent on the interface
0 RIP received, 1 RIP sent, 0 RIP discarded	IPX RIP packets received, sent, discarded
0 RIP specific requests received, 0 RIP specific responses sent	IPX RIP specific requests received, responses sent
0 RIP general requests received, 0 RIP general responses sent	IPX RIP general requests received, responses sent
0 SAP received, 0 SAP sent, 0 SAP discarded	Received, sent, discarded IPX SAP packets
0 SAP requests received, 0 SAP responses sent	Received IPX SAP packets, sent IPX SAP responses
IPX encapsulation	The IPX encapsulation format on the current interface

display ipx routing-table

Syntax **display ipx routing-table** [*network*]

View Any view

Parameter *Network:* Displays active routing information for the network.

Description Use the **display ipx routing-table** command to display active IPX routing information.

If no network is specified, all active routes are displayed.

Example # Display all active IPX routes.

```
<Sysname> display ipx routing-table
Routing tables:
Summary count: 1

Dest_Ntwk_ID    Proto  Pre Ticks Hops Nexthop           Interface
0x1         Direct 0   1     0    0.0000-0000-0000  Ethernt1/1
```

Table 659 Description on the fields of the display ipx routing-table command

Field	Description
Dest_Ntwk_ID	Destination network ID of the route
Proto	Protocol type of the route
Pre	Preference of the route
Ticks	Delay time of the route in ticks (a tick is 1/18 second)
Hops	Hop value of the route
Nexthop	The next hop of the route
Interface	Outgoing interface of the route

display ipx routing-table verbose

Syntax **display ipx routing-table** [*network*] **verbose**

View Any view

Parameter *Network:* Displays detailed routing information for the network, including both active and inactive routes.

Description Use the **display ipx routing-table verbose** command to display detailed IPX routing information, including active and inactive routes.

If no network is specified, all detailed IPX routing information is displayed.

Example # Display all detailed IPX routing information, including active and inactive routes.

```
<Sysname> display ipx routing-table verbose
Routing tables:
  Destinations: 2        Routes: 3
Destination Network ID: 0x1
          Protocol: Direct                    Preference: 0
          Ticks: 1                            Hops: 0
          Nexthop: 0.0000-0000-0000           Time: 0
          Interface: 1.0020-9c68-448e(Vlan-interface1)
          State: <Active>
          Protocol: Static                    Preference: -60
          Ticks: 1                            Hops: 1
          Nexthop: 2.000e-0001-0000           Time: 0
          Interface: 2.0020-9c68-448f(Vlan-interface2)
          State: <Inactive>
Destination Network ID: 0x2
          Protocol: Static                    Preference: 60
          Ticks: 1                            Hops: 1
          Nexthop: 1.000e-0001-0000           Time: 0
          Interface: 1.0020-9c68-448e(Vlan-interface1)
          State: <Active>
```

Table 660 Description on the fields of the display ipx routing-table verbose command

Field	Description
Destinations	Total number of destinations

Table 660 Description on the fields of the display ipx routing-table verbose command

Field	Description
Routes	Total number of routes
Destination Network ID	Destination network ID of the route
Protocol	Protocol type of the route
Preference	Preference of the route
Ticks	Delay time of the route in ticks (a tick is 1/18 second)
Hops	Hop value of the route
Nexthop	The next hop of the route
Time	Aging time of the route: 0 for directly connected routes and static routes, which do not age.
Interface	Address and name of the outbound interface
State	State of the route, which could be active or inactive

display ipx routing-table protocol

Syntax **display ipx routing-table protocol** { **default** | **direct** | **rip** | **static** } [**inactive** | **verbose**]

View Any view

Parameter **default**: Displays default routing information.

direct: Displays direct routing information.

rip: Displays all IPX RIP routing information.

static: Displays all IPX static routing information.

inactive: Displays inactive routing information.

verbose: Displays detailed routing information, including active and inactive routes.

Description Use the **display ipx routing-table protocol** command to display IPX routing information of the specified route types. Classified active and inactive routes are displayed if the **inactive** and **verbose** keywords are not specified.

Example # Display default IPX routing information.

```
<Sysname> display ipx routing-table protocol default
Default routing tables:
  Summary count: 0

Default routing tables status:<active>:
  Summary count: 0

Default routing tables status:<inactive>:
  Summary count: 0
display ipx routing-table statistics
```

display ipx routing-table statistics

Syntax **display ipx routing-table statistics**

View Any view

Parameter None

Description Use the **display ipx routing-table statistics** command to display IPX routing statistics.

Example # Display IPX routing statistics.

```
<Sysname> display ipx routing-table statistics
Routing tables:
Proto/State      route       active      added       deleted     freed
Direct           1           1           2           1           1
Static           2           1           2           0           0
RIP              0           0           0           0           0
Default          0           0           0           0           0

Total            3           2           4           1           1
```

Table 661 Description on the fields of the display ipx routing-table statistics command

Field	Description
Proto/State	Routing protocol
route	The number of routes, including active and inactive routes
active	Active routes
added	The number of added routes
deleted	The number of deleted routes
freed	The number of released routes

display ipx service-table

Syntax **display ipx service-table** [**inactive** | **name** *name* | **network** *network* | **order** { **network** | **type** } | **type** *service-type*] [**verbose**]

View Any view

Parameter **inactive**: Displays inactive service information.

name *name*: Displays the service information of a server. The name is a string of 1 to 47 characters.

network *network:* Displays service information on a network number which is a hexadecimal number in the range of 0x1 to 0xFFFFFFFF. Leading 0s can be omitted.

order { **network** | **type** }: Displays sorted service information. The **network** keyword indicates that information is sorted by network. The **type** keyword indicates that information is sorted by type.

type *service-type*: Displays information about a specified service type ID, which is in the range of 0x1 to 0xFFFF.

verbose: Displays detailed about service information.

Description Use the **display ipx service-table** command to display IPX service information.

If no parameters are specified, only active service information is displayed.

Example # Display active IPX service information.

```
<Sysname> display ipx service-table
Abbreviation: S - Static, Pref - Preference(Decimal), NetId - Network number,
NodeId - Node address, hop - Hops(Decimal), Recv-If - Interface from which the se
rvice is received

  Number of Static Entries:  2
  Number of Dynamic Entries: 0
  Name                                                Type      NetId
S Prn1                                                0005      000d
S Prn2                                                0005      0008
```

Display detailed IPX service information.

```
<Sysname> display ipx service-table verbose
Abbreviation: S - Static, Pref - Preference(Decimal), NetId - Network number,
NodeId - Node address, hop - Hops(Decimal), Recv-If - Interface from which the se
rvice is received

  Number of Static Entries:  2
  Number of Dynamic Entries: 0
  Name  Type      NetId NodeId          Sock     Pref Hops  Recv-If
S Prn1  0005      000d  000a-000a-000a  0452     500   02      Vlan-interface1
S Prn2  0005      0008  000a-000a-000a  0452     500   03      Vlan-interface1
```

Table 662 Description on the fields of the display ipx service-table command

Field	Description
Name	Server name
Type	Service type
NetId	Network ID
NodeId	Node ID
Sock	Socket
Pref	Preference
Hops	Hops to the server
Recv-If	Name of the receiving interface

display ipx statistics

Syntax **display ipx statistics**

View Any view

Parameter None

Description Use the **display ipx statistics** command to display IPX packet statistics.

Example # Display IPX packet statistics.

```
<Sysname> display ipx statistics
 Received: 0 total, 0 packets pitched
           0 packets size errors, 0 format errors
           0 bad hops(>16), 0 discarded(hops=16)
           0 other errors, 0 local destination
           0 can not be dealed
 Sent:     0 forwarded, 0 generated
           0 no route, 0 discarded
 RIP:      0 sent, 0 received
           0 responses sent, 0 responses received
           0 requests received, 0 requests dealt
           0 requests sent, 0 periodic updates
 SAP:      0 general requests received
           0 specific requests received
           0 GNS requests received
           0 general responses sent
           0 specific responses sent
           0 GNS responses sent
           0 periodic updates, 0 errors
 PING:     0 requests sent, 0 requests received
           0 responses sent, 0 responses received
           0 responses in time, 0 responses time out
```

Table 663 Description on the fields of the display ipx statistics command

Field	Description
Received: 0 total, 0 packets pitched 0 packets size errors, 0 format errors 0 bad hops(>16), 0 discarded(hops=16) 0 other errors, 0 local destination 0 can not be dealt with	Statistics of the received packets, including the total number of received packets, the number of padded packets, the number of packets with wrong packet size, the number of packets with encapsulation errors, the number of packets with a hop number greater than 16, the number of packets with hop number equal to 16, the number of other packets with errors, the number of packets with the destination set as the current device, the number of packets that cannot be processed.
Sent: 0 forwarded, 0 generated 0 no route, 0 discarded	Statistics of the sent packets, including the number of forwarded packets, the number of packets sent by the current device, the number of un-routable packets, and the number of discarded packets.
RIP: 0 sent, 0 received 0 responses sent, 0 responses received 0 requests received, 0 requests dealt 0 requests sent, 0 periodic updates	Statistics of RIP packets, including the total number of sent and received RIP packets, the number of sent and received response packets, the number of received, processed, and sent request packets, and the number of sent periodic update packets.

Table 663 Description on the fields of the display ipx statistics command

Field	Description
SAP: 0 general requests received 0 specific requests received 0 GNS requests received 0 general responses sent 0 specific responses sent 0 GNS responses sent 0 periodic updates, 0 errors	Statistics of SAP packets, including the number of received general request packets, the number of received specific request packets, the number of received GNS request packets, the number of sent general response packets, the number of sent specific response packets, the number of sent GNS packets, the number of sent packets with periodic updates, and the number of received error packets.
PING: 0 requests sent, 0 requests received 0 responses sent, 0 responses received 0 responses in time, 0 responses time out	Statistics of ping packets, including the number of sent and received request packets, the number of sent and received response packets, the number of packets responded in time, and the number of timeout response packets.

ipx enable

Syntax **ipx enable** [**node** *node*]

undo ipx enable

View System view

Parameter **node** *node*: Global node address of the router, used by all non-Ethernet interfaces. It is in 48-bit length, represented by a triplet of four-digit hexadecimal numbers separated by "-". It is neither a broadcast address nor a multicast address. If the argument is not specified, the router will assign the MAC address of the first Ethernet interface as the global node address. If there is no Ethernet interface in the router, then a node address will be randomly generated according to the system clock.

Description Use the **ipx enable** command to enable IPX.

Use the **undo ipx enable** command to disable IPX and remove all IPX configurations simultaneously.

IPX is disabled by default.

CAUTION: *Using the* ***undo ipx enable*** *command removes the previous IPX configuration.*

Example # Enable IPX.

```
<Sysname> system-view
[Sysname] ipx enable
```

ipx encapsulation

Syntax **ipx encapsulation** [**dot2** | **dot3** | **ethernet-2** | **snap**]

undo ipx encapsulation

View Interface view

Parameter **dot2**: Specifies the encapsulation format as Ethernet_802.2.

dot3: Specifies the encapsulation format as Ethernet_802.3.

ethernet-2: Specifies the encapsulation format as Ethernet_II.

snap: Specifies the encapsulation format as Ethernet_SNAP.

Description Use the **ipx encapsulation** command to specify an IPX frame encapsulation format for the current interface.

Use the **undo ipx encapsulation** command to restore the default IPX frame encapsulation format.

By default, IPX frame encapsulation format is **dot3** (Ethernet_802.3).

The command is only applicable to the layer 3 Ethernet interface and the VLAN interface.

Example # Specify the IPX frame encapsulation format on the interface 1/0 as Ethernet_II.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx encapsulation ethernet-2
```

ipx netbios-propagation

Syntax **ipx netbios-propagation**

undo ipx netbios-propagation

View Interface view

Parameter None

Description Use the **ipx netbios-propagation** command to enable the interface to forward the type 20 broadcast packets.

Use the **undo ipx netbios-propagation** command to disable the interface from forwarding the type 20 broadcast packets.

By default, type 20 broadcast packets are not forwarded.

Example # Enable Ethernet 1/0 to forward type 20 broadcast packets.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx netbios-propagation
```

ipx network

Syntax **ipx network** *network-number*

undo ipx network

View Interface view

Parameter *network-number*: IPX network ID in hexadecimal format. It ranges from 0x1 to 0xFFFFFFFD. Leading 0s can be omitted.

Description Use the **ipx network** command to configure a network ID for the interface.

Use the **undo ipx network** command to delete the IPX network ID of the interface.

By default, no network ID is allocated to an interface, that is, IPX is still disabled on the interface after IPX is enabled in system view.

Example # Assign network ID 675 to the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx network 675
```

ipx rip import-route static

Syntax **ipx rip import-route static**

undo ipx rip import-route static

View System view

Parameter **None**

Description Use the **ipx rip import-route static** command to enable static route redistribution into RIP. If successful, RIP routing updates will contain the redistributed static routes.

Use the **undo ipx rip import-route static** command to disable static route redistribution.

By default, IPX RIP does not redistribute static routes.

Note that RIP only redistributes active static routes, rather than inactive routes.

Example # Enable static route redistribution to RIP.

```
<Sysname> system-view
[Sysname] ipx rip import-route static
```

ipx rip mtu

Syntax **ipx rip mtu** *bytes*

undo ipx rip mtu

View Interface view

Parameter *bytes*: Maximum RIP updating packet size in bytes, ranging from 432 to 1,500.

Description Use the **ipx rip mtu** command to configure the maximum RIP updating packet size.

Use the **undo ipx rip mtu** command to restore the default.

The default is 432 bytes.

In RIP updating packets, the size of each routing information item is 8 bytes and the size of IPX header plus RIP header is 32 bytes. So an updating packet can carry up to 50 routing information items at most.

Example # Specify the maximum RIP updating packet size as 500 bytes on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx rip mtu 500
```

ipx rip multiplier

Syntax **ipx rip multiplier** *multiplier*

undo ipx rip multiplier

View System view

Parameter *multiplier*: Used to calculate the aging period of RIP routing items, ranging from 1 to 1000. The actual aging time is the value of *multiplier* multiplied by the RIP updating interval.

Description Use the **ipx rip multiplier** command to configure the aging interval of IPX RIP routing items.

Use the **undo ipx rip multiplier** command to restore the default.

The default is 3 times the update interval.

A timer is set for each routing entry to keep track of elapsed time since the route was received. Every time the updating packet containing the route is received, the timer is reset to zero. If a RIP route is not updated within the aging period, the system will regard the route as invalid and will delete it from the routing table.

Related command: **ipx rip timer update**.

Example # Configure the aging interval to be 5 times the update interval.

```
<Sysname> system-view
[Sysname] ipx rip multiplier 5
```

ipx rip timer update

Syntax **ipx rip timer update** *seconds*

undo ipx rip timer update

View System view

Parameter *seconds*: RIP updating interval in seconds, ranging from 10 to 60,000.

Description Use the **ipx rip timer update** command to specify a RIP update interval.

Use the **undo ipx rip timer update** command to restore the default.

The default update interval is 60 seconds.

Related command: **ipx rip multiplier**.

Example # Specify a RIP update interval of 30 seconds.

```
<Sysname> system-view
[Sysname] ipx rip timer update 30
```

ipx route-static

Syntax **ipx route-static** dest-*network* { *network.node* | *interface-type interface-number* } [**preference** *value*] [**tick** *ticks* **hop** *hops*]

undo ipx route-static { dest-*network* [*nexthop-addr* | *interface-type interface-number*] | **all** }

View System view

Parameter dest-*network*: Destination network ID of the IPX static route, an 8-digit hexadecimal number, ranging from 0x1 to 0xFFFFFFFE.

network.node: Next hop address of the IPX static route. *network* is an 8-digit hexadecimal number in the range 0x1 to 0xFFFFFFFD. The 48-bit *node* consists of three 4-digit hexadecimal numbers, separated by "-"; when entered, the leftmost 0s can be omitted.

interface-type interface-number: Type and number of the outgoing interface that must support PPP encapsulation. It can be a Serial or POS interface.

preference *value*: Route preference, in the range of 1 to 255. The smaller the value, the higher the preference. The preference of directly connected routes is fixed to 0 and cannot be changed. By default, the preference of IPX static routes is 60 and can be configured. The preference of dynamic IPX routes is fixed to 100 and cannot be changed.

tick *ticks*: Time needed to reach the destination network (1 tick = 1/18 second)., ranging from 1 to 65,534. The default is 1. When the tick value of the outgoing interface is modified, the tick value of the corresponding static route will also be changed. The *ticks* must be configured together with the *hops*.

hops: Number of routers on the route to the destination network, in the range 1 to 15. By default, the value is 1. It must be configured together with the *ticks* argument.

all: All IPX static routes.

Description Use the **ipx route-static** command to configure an IPX static route.

Use the **undo ipx route-static** command to remove an IPX static route.

The IPX static route with a destination network ID of 0xFFFFFFFE is the default route.

Example # Configure an IPX static route with destination network ID being 0x5a, the next hop being 1000.0-0c91-f61f, ticks 10 and hops 2.

```
<Sysname> system-view
[Sysname] ipx route-static 5a 1000.0-0c91-f61f tick 10 hop 2
```

ipx route load-balance-path

Syntax **ipx route load-balance-path** *paths*

undo ipx route load-balance-path

View System view

Parameter *paths*: Maximum number of equivalent routes for load balancing, ranging from 1 to 64.

Description Use the **ipx route load-balance-path** command to specify the maximum number of equivalent routes to the same destination.

Use the **undo ipx route load-balance-path** command to restore the default.

The default is 1.

This number is the maximum active equivalent route number of the system. If a newly configured number is smaller than the previous, the system will change the excessive active routes to inactive routes.

Example # Specify the maximum equivalent route number to the same destination address as 30.

```
<Sysname> system-view
[Sysname] ipx route load-balance-path 30
```

ipx route max-reserve-path

Syntax **ipx route max-reserve-path** *paths*

undo ipx route max-reserve-path

View System view

Parameter *paths*: Maximum number of routes to the same destination, including both static and dynamic routes, in the range 1 to 255.

Description Use the **ipx route max-reserve-path** command to specify the maximum number of routes to the same destination.

Use the **undo ipx route max-reserve-path** command to restore the default.

By default, the value is 4.

When the route number to the same destination address exceeds the maximum value configured, the newly found dynamic routes will not be added into the routing table, but discarded directly. If the newly configured value is less than the original one, the excessive routes in the current routing table will not be deleted until they get aged out or are deleted manually.

Example # Specify the maximum number of routes to the same destination to 200.

```
<Sysname> system-view
[Sysname] ipx route max-reserve-path 200
```

ipx sap disable

Syntax **ipx sap disable**

undo ipx sap disable

View Interface view

Parameter None

Description Use the **ipx sap disable** command to disable IPX SAP on the current interface.

Use the **undo ipx sap disable** command to enable IPX SAP on the current interface.

By default, the SAP is enabled on the interface after IPX is enabled.

Example # Disable SAP on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx sap disable
```

ipx sap gns-disable-reply

Syntax **ipx sap gns-disable-reply**

undo ipx sap gns-disable-reply

View Interface view

Parameter None

Description Use the **ipx sap gns-disable-reply** command to disable the interface from responding to IPX GNS requests.

Use the **undo ipx sap gns-disable-reply** command to enable the interface to respond to IPX GNS requests.

By default, an interface is capable of responding to GNS requests.

Example # Disable Ethernet 1/0 from responding to IPX GNS requests.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx sap gns-disable-reply
```

ipx sap gns-load-balance

Syntax **ipx sap gns-load-balance**

undo ipx sap gns-load-balance

View System view

Parameter None

Description Use the **ipx sap gns-load-balance** command to configure the router to respond to GNS requests in the Round-robin method.

Use the **undo ipx sap gns-load-balance** command to configure the router to respond with the nearest server.

By default, the Round-Robin mode is used, that is, the router informs the clients of servers in turn lest a server shoulders too much pressure.

Related command: **ipx sap gns-disable-reply**.

Example # Configure the router to respond to clients with the nearest server.

```
<Sysname> system-view
[Sysname] undo ipx sap gns-load-balance
```

ipx sap max-reserve-servers

Syntax **ipx sap max-reserve-servers** *length*

undo ipx sap max-reserve-servers

View System view

Parameter *length*: Maximum reserve queue length of the same type service information, ranging from 1 to 2,048.

Description Use the **ipx sap max-reserve-servers** command to specify the maximum reserve queue length of the same type service information.

Use the **undo ipx sap max-reserve-servers** command to restore the default.

By default, the value is 2,048.

If a newly configured value is smaller than the previous one, the excessive items in the service information table (SIT for short) will not be deleted. If the service information item number for the same service type exceeds the maximum value, new service information will not be added.

Example # Set the maximum reserve queue length of the same type service information to 1,024.

```
<Sysname> system-view
[Sysname] ipx sap max-reserve-servers 1024
```

ipx sap mtu

Syntax **ipx sap mtu** *bytes*

undo ipx sap mtu

View Interface view

Parameter *bytes*: Maximum SAP packet size in bytes, ranging from 480 to 1,500.

Description Use the **ipx sap mtu** command to configure the maximum size of SAP updating packets.

Use the **undo ipx sap mtu** command to restore the default.

By default, the value is 480 bytes. The size of the IPX header plus SAP header is 32 bytes, so a 480-byte SAP updating packet contains 7 service information items (64 bytes each).

Example # Set the maximum size of SAP updating packets on the interface Ethernet1/0 to 674 bytes (10 service information items at most).

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx sap mtu 674
```

ipx sap multiplier

Syntax **ipx sap multiplier** *multiplier*

undo ipx sap multiplier

View System view

Parameter *multiplier*: Value multiplied by the updating interval to yield the aging interval for SAP service information items. The value ranges from 1 to 1000.

Description Use the **ipx sap multiplier** command to configure the aging interval of SAP service information items.

Use the **undo ipx sap multiplier** command to restore the default.

The default aging time is three times the IPX SAP update interval.

Related command: **ipx sap timer update**.

Example # Set the aging interval of SAP service information items to be 5 times the updating interval.

```
<Sysname> system-view
[Sysname] ipx sap multiplier 5
```

ipx sap timer update

Syntax **ipx sap timer update** *seconds*

undo ipx sap timer update

View System view

Parameter *seconds*: SAP updating interval, ranging from 10 to 60,000 seconds.

Description Use the **ipx sap timer update** command to specify the IPX SAP updating interval.

Use the **undo ipx sap timer update** command to restore the default.

By default, the update interval is 60 seconds.

Using this command does not take effect on an interface that adopts triggered update.

Related command: **ipx sap multiplier**, **ipx update-change-only**.

Example # Specify the SAP updating interval as 300 seconds.

```
<Sysname> system-view
[Sysname] ipx sap timer update 300
```

ipx service

Syntax **ipx service** *service-type server-name network.node socket* **hop** *hopcount* [**preference** *preference*]

undo ipx service { *service-type* [*server-name* [*network.node*]] [**preference** *preferenc*e] | **all** }

View System view

Parameter *service-type*: Service type, ranging from 0 to 0xFFFF. A value of 0 indicates all service types.

server-name: Name of the server which provides the service, a string of 1 to 47 characters.

network.node: Network ID and node ID of a server. Network ID is an 8-bit hexadecimal number, ranging from 0x1 to 0xFFFFFFFD. Node ID has a length of 48 bits, represented by a triplet of 4-digit hexadecimal numbers separated by "-". Leading 0s can be omitted.

socket: It is a 4-bit hexadecimal number, ranging from 0x1 to 0xFFFF.

hop *hop-count*: Number of hops to reach the server, ranging from 1 to 15. Note that hop count more than or equal to 16 implies the service is unreachable.

preference *preference*: Preference of service information, ranging from 1 to 255. The smaller the value, the higher the preference. By default, the preference of the static service information items is 60 and is configurable, and the preference of the dynamic items is 500 and cannot be configured.

all: Deletes all static service information items.

Description Use the **ipx service** command to add an IPX static service information item.

Use the **undo ipx service** command to delete an IPX static service information item.

Example # Add a static service information item with the service type being 4, service name "FileServer", server network ID 130, node value 0000-0a0b-abcd, server hop 1 and server preference 60.

```
<Sysname> system-view
[Sysname] ipx service 4 FileServer 130.0000-0a0b-abcd 451 hop 1 preference 60
```

ipx split-horizon

Syntax **ipx split-horizon**

undo ipx split-horizon

View Interface view

Parameter None

Description Use the **ipx split-horizon** command to enable split horizon on the current interface.

Use the **undo ipx split-horizon** command to disable split horizon on the current interface.

By default, split horizon is enabled on the interface.

Example # Enable split horizon on the interface Ethernet1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx split-horizon
```

ipx tick

Syntax **ipx tick** *ticks*

undo ipx tick

View Interface view

Parameter *ticks*: Delay in ticks, ranging from 0 to 30,000. One tick is 1/18 second (approximately 55 ms).

Description Use the **ipx tick** command to specify a delay for sending IPX packets on the interface.

Use the **undo ipx tick** command to restore the default.

By default, the delay on an Ethernet or a VLAN interface is 1 tick, that on an asynchronous serial port is 30 ticks, and that on a synchronous serial port is 6 ticks.

Example # Configure the delay for sending IPX packets as 5 ticks on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx tick 5
```

ipx update-change-only

Syntax **ipx update-change-only**

undo ipx update-change-only

View Interface view

Parameter None

Description Use the **ipx update-change-only** command to enable the triggered update feature on the current interface.

Use the **undo ipx update-change-only** command to disable the triggered update feature on the current interface.

By default, the triggered update feature is disabled on an interface.

Example # Enable the triggered update feature on the interface Ethernet 1/0.

```
<Sysname> system-view
[Sysname] interface ethernet 1/0
[Sysname-Ethernet1/0] ipx update-change-only
```

ping ipx

Syntax **ping ipx** *network.node* [**-c** *count* | **-t** *timeout* | **-s** *size*] *

View Any view

Parameter *network.node*: Destination address. The argument *network* is an eight-bit hexadecimal number ranging from 0x1 to 0xFFFFFFFD. The argument *node* is a 48-bit value represented by a triplet of four-digit hexadecimal numbers separated by "-". The 0s in front can be omitted when inputting.

-c *count*: Number of ping packets to be sent. By default, the value is 5. This value ranges from 1 to 4,294,967,295.

-t *timeout*: Timeout interval of ping packets in milliseconds. By default, the value is 2 milliseconds. This value ranges from 0 to 65,535.

-s *size*: Ping packet size, in bytes. By default, the value is 100 bytes. This value ranges from 44 to 1,500.

Description Use the **ping ipx** command to check host reachability and network connectivity in an IPX network.

Example # Ping the destination address at 675.0000-a0b0-fefe.

```
<Sysname> ping ipx 675.0000-a0b0-fefe
```

reset ipx statistics

Syntax **reset ipx statistics**

View User view

Parameter None

Description Use the **reset ipx statistics** command to clear IPX statistics.

Example # Clear IPX statistics.

```
<Sysname> reset ipx statistics
```

reset ipx routing-table statistics protocol

Syntax **reset ipx routing-table statistics protocol** [**all** | **default** | **direct** | **rip** | **static**]

View User view

Parameter *all:* Clears the statistics of IPX routes of all types.

default: Clears the statistics of the default IPX route.

direct: Clears the statistics of the direct IPX routes.

rip: Clears the statistics of the IPX RIP routes.

static: Clears the statistics of the static IPX routes.

Description Use the **reset ipx routing-table statistics protocol** command to clear the statistics of a specified IPX route type.

Related command: **display ipx routing-table statistics**.

Example # Display IPX routing statistics.

```
<Sysname> display ipx routing-table statistics
Routing tables:
Proto/State      route       active      added       deleted     freed
Direct           1           1           1           0           0
Static           9           9           14          5           5
RIP              0           0           0           0           0
Default          0           0           0           0           0

Total            10          10          15          5           5
```

Clear IPX static route statistics.

```
<Sysname> reset ipx routing-table statistics protocol static
This will erase the specific routing counters information.
Are you sure?[Y/N]y
<Sysname>
```

Display IPX routing statistics again and you can see the following changes.

```
<Sysname>dis ipx routing-table statistics
Routing tables:
Proto/State      route       active      added       deleted     freed
Direct           1           1           1           0           0
Static           9           9           0           0           0
RIP              0           0           0           0           0
Default          0           0           0           0           0


Total            10          10          1           0           0
```

173 VoIP Configuration Commands

The voice subscriber line in this chapter refers to a digital or analog subscriber line, unless otherwise specified.

address

Syntax **address** { **ip** *ip-address* | **ras** | **sip** { **ip** *ip-address* [**port** *port-number*] | **proxy** } }

undo address { **ip** | **ras** | **sip** { **ip** | **proxy** } }

View VoIP entity view

Parameter **ip** *ip-address*: IP address of the terminating gateway, namely, the destination address of a VoIP entity.

ras: Uses RAS messages to interact with the GK server so as to find the mapping between the phone number and the IP address. They are used only in the networking configuration that uses a gatekeeper (GK) to provide IP voice services.

sip: Uses the SIP.

port *port-number*: Port number, in the range of 1 to 65535. The default port number is 5060.

proxy: Uses the SIP proxy server to implement SIP message exchange.

Description Use the **address** command to configure a policy for the routing between the VoIP entity and the terminating voice gateway.

Use the **undo address** command to remove the routing policy that has been configured.

By default, no policy is configured for routing from the VoIP entity to the peer VoIP gateway.

Related command: **match-template**.

Example # Configure the H.323 direct routing for voice entity 10 with the called number 1234 in its match template, and set the IP address of the terminating gateway to 10.1.1.2.

```
<Sysname> system-view
[Sysname] voice-setup
```

```
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] match-template 12345
[Sysname-voice-dial-entity10] address ip 10.1.1.2
```

area

Syntax **area** { **custom** | **europe** | **north-america** }

undo area

View Voice view

Parameter **custom**: Busy tone defined by users.

europe: Busy tone compliant with Europe standard.

north-america: Busy tone compliant with North America standard.

Description Use the **area** command to configure the type of busy tone for FXO voice subscriber line.

Use the **undo area** command to restore the default type.

By default, the busy tone compliant with the Europe standard is used.

This command applies to 2-wire loop trunk subscriber line FXO only. Once this command is configured, the configuration will be effective to all the analog FXO voice cards on the device.

When an FXO interface card is connected to a common subscriber line of a program-controlled switch, if the user on the switch side hangs up first, only by detecting the busy tone can the router know that the user has hung up. This is made possible because different switches adopt different cptone schemes with varying frequency spectrum characteristics, based on which the busy tone can be identified.

Example # Configure the busy tone type compliant with the North America standard.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] area north-america
```

area-id

Syntax **area-id** *string*

undo area-id

View VoIP/VoFR entity view

Parameter *string:* Area ID, a string of 1 to 31 characters, which consists of digits 0 through 9 and the pound sign #.

Description Use the **area-id** command to configure the area ID of the voice GW.

Use the **undo area-id** command to remove the specified area ID.

By default, no area ID is configured.

The voice area ID is set in VoIP entity view and will be automatically added to the beginning of called numbers when making calls. If SIP is specified for routing, this command is invalid.

Related command: **match-template**, **address**, and **entity**.

Example # Configure the area ID 6# for the VoIP voice entity 101.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 101 voip
[Sysname-voice-dial-entity101] area-id 6#
```

busytone-t-th

Syntax **busytone-t-th** *time-threshold*

undo busytone-t-th

View Analog FXO voice subscriber line view

Parameter *time-threshold*: Number of busy tone periods for detection, in the range of 2 to 12. A bigger value means a longer busy tone detection time.

Description Use the **busytone-t-th** command to configure the number of busy tone periods for detection.

Use the **undo busytone-t-th** command to restore the default.

By default, the number of busy tone periods for detection is 2.

You can enable the busy tone detection optionally. Under particular situations, however, the actual busy tone data cannot exactly match the busy tone parameters configured for the system. If there is a big difference, the busy tone may not be detected correctly, resulting in on-hook failures or wrong on-hooks. By adjusting the time threshold of busy tone detection, you make the busy tone detection more precise.

Note that before you configure a threshold of busy tone detection, you must test it fully making sure that on-hook operation can be done properly.

Example # Set the number of busy tone periods to 3.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] busytone-t-th 3
```

cid display

Syntax **cid display**

undo cid display

View Analog FXS voice subscriber line view

Parameter None

Description Use the **cid display** command to enable caller identity delivery (CID) on an analog FXS voice subscriber line.

Use the **undo cid display** command to disable CID.

By default, CID is enabled on an analog FXS voice subscriber line.

Example # Enable CID on voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] cid display
```

cid receive

Syntax **cid receive**

undo cid receive

View Analog FXO voice subscriber line view

Parameter None

Description Use the **cid receive** command to enable CID.

Use the **undo cid enable** command to disable CID.

By default, CID is enabled.

When CID is disabled, the local FXO interface does the following when the calling party sends a calling number:

- If a number is configured in the number template for the POTS entity associated with the local FXO interface, the interface substitutes this number for the calling number and sends it to the called side.
- If wildcard dots (.) are used in the number configured in the number template for the POTS entity associated with the local FXO interface, the interface substitutes zeros for the calling number's digits in the place of dots, for example, 1000 for 1... and then sends the substitution number to the called side.

Example # Enable CID on voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] cid receive
```

cid send

Syntax **cid send**

undo cid send

View FXS/FXO voice subscriber line view

Parameter None

Description Use the **cid send** command to enable the FXS or FXO voice subscriber line to send calling numbers to the remote end.

Use the **undo cid send** command to disable the FXS or FXO voice subscriber line from send calling numbers to the remote end.

By default, the FXS or FXO voice subscriber line sends calling numbers to the remote end.

After you configure the **undo cid send** command, the FXS or FXO voice subscriber line will not send any calling number to the called side, whether the originating side has sent it or it is configured in the number template for the voice entity associated with the FXS or FXO voice subscriber line.

Example # Disable voice subscriber line 1/0 from sending calling numbers to the IP network.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] undo cid send
```

cid type

Syntax **cid type** { **complex** | **simple** }

undo cid type

View Analog FXS voice subscriber line view

Parameter **complex**: Caller identification information is transmitted in multiple-data message format (MDMF).

simple: Caller identification information is transmitted in single-data message format (SDMF).

Description Use the **cid type** command to configure the format of message (which carries the calling number information) transmitted over the FXS voice subscriber line.

Use the **undo cid type** command to restore the default message format.

By default, the multiple data message format (MDMF) is adopted.

Two formats are available: multiple data message format (MDMF) and single data message format (SDMF). If the remote end supports one format only, you must use the same message format at the local end.

Example # Set the format of the transmitted caller identification information to SDMF on voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] cid type simple
```

cng-on

Syntax **cng-on**

undo cng-on

View FXS/FXO/E&M voice subscriber line view

Parameter None

Description Use the **cng-on** command to enable comfortable noise function.

Use the **undo cng-on** command to disable this function.

By default, the comfortable noise function is enabled.

This command is applicable to FXO, FXS, E&M subscriber lines and E1/T1 voice subscriber line.

You can use this command to generate some comfortable background noise to replace the toneless intervals during a conversation. If no comfortable noise is

generated, the toneless intervals will make both parties in conversation feel uncomfortable.

Related command: **line** and **vad-on**.

Example # Disable comfortable noise function on subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] undo cng-on
```

compression

Syntax **compression** { **1st-level | 2nd-level | 3rd-level | 4th-level** } { **g711alaw | g711ulaw | g723r53 | g723r63 | g726r16 | g726r24 | g726r32 | g726r40 | g729a | g729r8** }

undo compression { **1st-level** | **2nd-level** | **3rd-level** | **4th-level** }

View POTS/VoIP/VoFR entity view

Parameter **1st-level**: Specifies a codec with the first priority.

2nd-level: Specifies a codec with the second priority.

3rd-level: Specifies a codec with the third priority.

4th-level: Specifies a codec with the fourth priority (namely, the lowest priority).

g711alaw: G.711 A-law codec (defining the pulse code modulation technology), requiring a bandwidth of 64 kbps, usually adopted in Europe.

g711ulaw: G.711μ-law codec, requiring a bandwidth of 64 kbps, usually adopted in North America and Japan.

g723r53: G.723.1 Annex A codec, requiring a bandwidth of 5.3 kbps.

g723r63: G.723.1 Annex A codec, requiring a bandwidth of 6.3 kbps.

g726r16: G.726 Annex A codec. It uses the adaptive differential pulse code modulation (ADPCM) technology, requiring a bandwidth of 16 kbps.

g726r24: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 24 kbps. The support for the **g726r24** keyword varies with devices.

g726r32: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 32 kbps. The support for the **g726r32** keyword varies with devices.

g726r40: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 40 kbps. The support for the **g726r40** keyword varies with devices.

g729a: G.729 Annex A codec (a simplified version of G.729), requiring a bandwidth of 8 kbps.

g729r8: G.729 (the voice compression technology using conjugate algebraic-code-excited linear-prediction), requiring a bandwidth of 8 kbps.

Description

Use the **compression** command to configure the voice compression method and the preference level.

Use the **undo compression** command to restore the default value.

By default, the codec with the first priority is **g729r8**, that with the second priority is **g711alaw**, that with the third priority is **g711ulaw**, and that with the fourth priority is **g723r53**.

g711alaw and **g711ulaw** provide high-quality voice transmission, while requiring greater bandwidth.

g723r53 and **g723r63** provide silence suppression technology and comfortable noise, the relatively higher speed output is based on multi-pulse multi-quantitative level technology and provides relatively higher voice quality to certain extent, and the relatively lower speed output is based on the Algebraic-Code-Excited Linear-Prediction technology and provides greater flexibility for application.

The voice quality provided by **g729r8** and **g729a** is similar to the ADPCM of 32 kbps, having the quality of a toll, and also featuring low bandwidth, lesser event delay and medium processing complexity, hence it has a wide field of application.

Table 664 describes the relationship between codec algorithms and bandwidth.

Table 664 Relationship between algorithms and bandwidth

Codec	Bandwidth	Voice quality
G.711 (A-law and μ-law)	64 kbps (without compression)	Best
G.726	16, 24, 32, 40 kbps	Good
G.729	8 kbps	Good
G.723 r63	6.3 kbps	Fair
G.723 r53	5.3 kbps	Fair

Actual network bandwidth is related to packet assembly interval and network structure. The longer the packet assembly interval is, the closer the network bandwidth is to the media stream bandwidth. More headers consume more bandwidth. Longer packet assembly interval results in longer fixed coding latency.

The following tables show the relevant packet assembly parameters without IPHC compression, including packet assembly interval, bytes coded in a time unit, and network bandwidth, etc. Thus, you can choose a suitable codec algorithm according to idle and busy status of the line and network situations more conveniently.

Table 665 G.711 algorithm (A-law and μ-law)

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes)IP+ PPP	Network bandwidth IP+PPP	Coding latency
10 ms	80	120	96 kbps	126	100.8 kbps	10 ms
20 ms	160	200	80 kbps	206	82.4 kbps	20 ms
30 ms	240	280	74.7 kbps	286	76.3 kbps	30 ms
G.711 algorithm (A-law and μ-law): media stream bandwidth 64kbps, minimum packet assembly interval 10 ms.						

Table 666 G.723 r63 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes)IP+ PPP	Network bandwidth IP+PPP	Coding latency
30 ms	24	64	16.8 kbps	70	18.4 kbps	30 ms
60 ms	48	88	11.6 kbps	94	12.3 kbps	60 ms
90 ms	72	112	9.8 kbps	118	10.3 kbps	90 ms
G.723 r63 algorithm: media stream bandwidth 6.3 kbps, minimum packet assembly interval 30 ms.						

Table 667 G.723 r53 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
30 ms	20	60	15.9 kbps	66	17.5 kbps	30 ms
60 ms	40	80	10.6 kbps	86	11.4 kbps	60 ms
90 ms	60	100	8.8 kbps	106	9.3 kbps	90 ms
G.723 r53 algorithm: media stream bandwidth 5.3 kbps, minimum packet assembly interval 30 ms.						

Table 668 G.726 r16 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
10 ms	20	60	48 kbps	66	52.8 kbps	10 ms
20 ms	40	80	32 kbps	86	34.4 kbps	20 ms
30 ms	60	100	26.7 kbps	106	28.3 kbps	30 ms
40 ms	80	120	24 kbps	126	25.2 kbps	40 ms
50 ms	100	140	22.4 kbps	146	23.4 kbps	50 ms
60 ms	120	160	21.3 kbps	166	11.4 kbps	60 ms
70 ms	140	180	20.6 kbps	186	21.3 kbps	70 ms
80 ms	160	200	20 kbps	206	20.6 kbps	80 ms
90 ms	180	220	8.8 kbps	226	9.3 kbps	90 ms
100 ms	200	240	19.2 kbps	246	19.7 kbps	100 ms

Table 668 G.726 r16 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
110 ms	220	260	18.9 kbps	266	19.3 kbps	110 ms
G.726 r16 algorithm: media stream bandwidth 16 kbps, minimum packet assembly interval 10 ms.						

Table 669 G.726 r24 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
10 ms	30	70	56 kbps	76	60.8 kbps	10 ms
20 ms	60	100	40 kbps	106	42.4 kbps	20 ms
30 ms	90	130	34.7 kbps	136	17.5 kbps	30 ms
40 ms	120	160	32 kbps	166	33.2 kbps	40 ms
50 ms	150	190	30.4 kbps	196	31.2 kbps	50 ms
60 ms	180	220	29.3 kbps	226	11.4 kbps	60 ms
70 ms	210	250	28.6 kbps	256	30.1 kbps	70 ms
G.726 r24 algorithm: media stream bandwidth 24 kbps, minimum packet assembly interval 10 ms.						

Table 670 G.726 r32 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
10 ms	40	80	64 kbps	86	68.8 kbps	10 ms
20 ms	80	120	48 kbps	126	50.4 kbps	20 ms
30 ms	120	160	42.7 kbps	166	44.3 kbps	30 ms
40 ms	160	200	40 kbps	206	41.2 kbps	40 ms
50 ms	200	240	38.4 kbps	246	39.4 kbps	50 ms
G.726 r32 algorithm: media stream bandwidth 32 kbps, minimum packet assembly interval 10 ms.						

Table 671 G.726 r40 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
10 ms	50	90	72 kbps	96	76.8 kbps	10 ms
20 ms	100	140	56 kbps	146	58.4 kbps	20 ms
30 ms	150	190	50.7 kbps	196	52.3 kbps	30 ms
40 ms	200	240	48 kbps	246	49.2 kbps	40 ms
G.726 r40 algorithm: media stream bandwidth 40 kbps, minimum packet assembly interval 10 ms.						

Table 672 G.729 algorithm

Packet assembly interval	Bytes coded in a time unit	Packet length (bytes) IP	Network bandwidth IP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Coding latency
10 ms	10	50	40 kbps	56	44.8 kbps	10 ms
20 ms	20	60	24 kbps	66	26.4 kbps	20 ms
30 ms	30	70	18.7 kbps	76	20.3 kbps	30 ms
G.729 algorithm: media stream bandwidth 8 kbps, minimum packet assembly interval 10 ms.						

- *Packet assembly interval is the duration to encapsulate information into a voice packet.*
- *Bytes coded in a time unit = packet assembly interval X media stream bandwidth.*
- *Packet length (IP) = IP header + RTP header + UDP header + voice information length = 20+12+8+data*
- *Packet length (IP+PPP) = PPP header + IP header + RTP header + UDP header + voice information length = 6+20+12+8+data*
- *Network bandwidth = Bandwidth of the media stream X packet length / bytes coded in a time unit*

Since IPHC compression is affected significantly by network stability, it cannot achieve high efficiency unless line is of high quality, network is very stable, and packet loss does not occur or seldom occurs. When the network is unstable, IPHC efficiency drops drastically. With best IPHC performance, IP (RTP) header can be compressed to 2 bytes. If PPP header is compressed at the same time, a great deal of media stream bandwidth can be saved. The following table shows the best IPHC compression efficiency of codec algorithms with packet assembly interval of 30ms.

Table 673 Compression efficiency of IPHC+PPP header

		Before compression		After IPHC+PPP compression	
Codec	Bytes coded in a time unit	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP	Packet length (bytes) IP+PPP	Network bandwidth IP+PPP
G.729	30	76	20.3 kbps	34	9.1 kbps
G.723r63	24	70	18.4 kbps	28	7.4 kbps
G.723r53	20	66	17.5 kbps	24	6.4 kbps
G.726r16	60	106	28.3 kbps	64	17.1 kbps
G.726r24	90	136	17.5 kbps	94	25.1 kbps
G.726r32	120	166	44.3 kbps	124	33.1 kbps
G.726r40	150	196	52.3 kbps	154	41.1 kbps

Two communication parties can communicate normally only if they share some identical coding/decoding algorithms. If the codec algorithm between two connected devices is not consistent, or the two devices share no common coding/decoding algorithms, the calling will fail.

Example # Configure to use g723r53 coding/decoding algorithm first, then the g729r8.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] compression 1st-level g723r53
[Sysname-voice-dial-entity10] compression 2nd-level g729r8
```

cptone country-type

Syntax **cptone country-type** *locale*

undo cptone country-type

View Voice view

Parameter **country type** *locale*: Configure the current device to play the call progress tones of a specified country or regions. Currently, call progress tones of 64 countries or regions are supported.

Table 674 Countries or regions with supported call progress tones

Code	Country name (including customization)
AR	Argentina
AU	Australia
AT	Austria
BE	Belgium
BR	Brazil
BG	Bulgaria
CA	Canada
CL	Chile
CN	China
CS	Customizes the call progress tones
HR	Croatia
CU	Cuba
CY	Cyprus
CZ	Czech Republic
DK	Denmark
EG	Egypt
FI	Finland
FR	France
DE	Germany
GH	Ghana
GR	Greece
HK	Hong Kong China
HU	Hungary
IS	Iceland

Table 674 Countries or regions with supported call progress tones

Code	Country name (including customization)
IN	India
ID	Indonesia
IR	Iran
IE	Ireland
IEU	Ireland (UK style)
IL	Israel
IT	Italy
JP	Japan
JO	Jordan
KE	Kenya
KR	Korea Republic
LB	Lebanon
LU	Luxembourg
MO	Macau
MY	Malaysia
MX	Mexico
NP	Nepal
NL	Netherlands
NZ	New Zealand
NG	Nigeria
NO	Norway
PK	Pakistan
PA	Panama
PH	Philippines
PL	Poland
PT	Portugal
RU	Russian Federation
SA	Saudi Arabia
SG	Singapore
SK	Slovakia
SI	Slovenia
ZA	South Africa
ES	Spain
SE	Sweden
CH	Switzerland
TH	Thailand
TR	Turkey
GB	United Kingdom
US	United States
UY	Uruguay
ZW	Zimbabwe

Description Use the **cptone country-type** command to configure the current device to play the call progress tones of a specified country or region or play the customized call progress tones.

Use the **undo cptone country-type** command to restore the default.

By default, the call progress tones of China are specified.

CAUTION: *The configuration of the* ***cptone country-type*** *command will take effect on all voice interfaces of all cards on the device.*

Example # Configure the device to play the call progress tones of US.

```
<sysname> system-view
[sysname] voice-setup
[sysname-voice] cptone country-type us
```

cptone tone-type

Syntax **cptone tone-type** { **all** | **busy-tone | congestion-tone | dial-tone | ringback-tone | special-dial-tone | waiting-tone** } **amplitude** *value*

undo cptone tone-type { **all** | **busy-tone | congestion-tone | dial-tone | ringback-tone | special-dial-tone | waiting-tone** } **amplitude**

View Voice view

Parameter **all**: All types of call progress tones.

busy-tone: Busy tone.

congestion-tone: Congestion tone.

dial-tone: Dial tone.

ringback-tone: Ringback tone.

special-dial-tone: Special dial tone.

waiting-tone: Call waiting tone.

amplitude *value*: Specifies the amplitude of a progress tone, which ranges from 200 to 1,500.

Description Use the **cptone tone-type** command to configure the amplitude of the specified call progress tones.

Use the **undo cptone tone-type** command to restore the default.

By default, the amplitude of busy tone and congestion tone is 1000, that of dial tone and special dial tone is 400, and that of ringback tone and call waiting tone is 600.

Example Set the amplitude of the busy tone to 1,200.

```
<sysname> system-view
[sysname] voice-setup
[sysname-voice] cptone tone-type busy-tone amplitude 1200
```

default entity compression

Syntax **default entity compression** { **1st-level** | **2nd-level** | **3rd-level** | **4th-level** } { **g711alaw** | **g711ulaw** | **g723r53** | **g723r63** | **g726r16** | **g726r24** | **g726r32** | **g726r40** | **g729a** | **g729r8** }

undo default entity compression { **1st-level** | **2nd-level** | **3rd-level** | **4th-level** }

View Voice dial program view

Parameter **1st-level**: Specifies a codec with the first priority.

2nd-level: Specifies a codec with the second priority.

3rd-level: Specifies a codec with the third priority.

4th-level: Specifies a codec with the fourth priority (namely, the lowest priority).

g711alaw: G.711 A-law codec (defining the pulse code modulation technology), requiring a bandwidth of 64 kbps, usually adopted in Europe.

g711ulaw: G.711μ-law codec, requiring a bandwidth of 64 kbps, usually adopted in North America and Japan.

g723r53: G.723.1 Annex A codec, requiring a bandwidth of 5.3 kbps.

g723r63: G.723.1 Annex A codec, requiring a bandwidth of 6.3 kbps.

g726r16: G.726 Annex A codec. It uses the adaptive differential pulse code modulation (ADPCM) technology, requiring a bandwidth of 16 kbps.

g726r24: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 24 kbps.

g726r32: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 32 kbps.

g726r40: G.726 Annex A codec. It uses ADPCM, requiring a bandwidth of 40 kbps.

g729a: G.729 Annex A codec (a simplified version of G.729), requiring a bandwidth of 8 kbps.

g729r8: G.729 (the voice compression technology using conjugate algebraic-code-excited linear-prediction), requiring a bandwidth of 8 kbps.

Description Use the **default entity compression** command to globally configure a default codec.

Use the **undo default entity compression** command to remove the configuration.

By default, the codec with the first priority is **g729r8**, that with the second priority is **g711alaw**, that with the third priority is **g711ulaw**, and that with the fourth priority is **g723r53**.

The **default entity compression** command can be used to globally configure the default mode of the voice coding and decoding. After the configuration, all the voice entities and newly created voice entities on this router, which have not been configured with this function, will inherit this configuration.

Related command: **compression**.

Example # Adopt the **g723r53** coding and decoding mode as the first selection globally.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] default entity compression 1st-level g723r53
```

default entity payload-size

Syntax **default entity payload-size** { **g711** | **g723** | **g726r16** | **g726r24** | **g726r32** | **g726r40** | **g729** } *time-length*

undo default entity payload-size { **g711** | **g723** | **g726r16** | **g726r24** | **g726r32** | **g726r40** | **g729** }

View Voice dial program view

Parameter **g711**: Specifies the packetization period for g711 codec. It can be 10, 20 (the default), or 30 milliseconds.

g723: Specifies the packetization period for g723 codec. It is an integral multiple of 30 in the range 30 to 180 milliseconds. It defaults to 30 milliseconds.

g726r16: Specifies the packetization period for g726r16 codec. It ranges from 10 to 110 milliseconds and defaults to 30 milliseconds.

g726r24: Specifies the packetization period for g726r24 codec. It ranges from 10 to 70 milliseconds and defaults to 30 milliseconds.

g726r32: Specifies the packetization period for g726r32 codec. It ranges from 10 to 50 milliseconds and defaults to 30 milliseconds.

g726r40: Specifies the packetization period for g726r40 codec. It ranges from 10 to 40 milliseconds and defaults to 30 milliseconds.

g729: Specifies the packetization period for g729 codec. It ranges from10 to 180 milliseconds and defaults to 30 milliseconds.

time-length: Packetization period for a codec.

Description Use the **default entity payload-size** command to configure the default packetization period for a codec.

Use the **undo default entity payload-size** command to restore the default.

Example # Set the packetization period for G.711 codec to 30 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] default entity payload-size g711 30
```

default entity vad-on

Syntax **default entity vad-on**

undo default entity vad-on

View Voice dial program view

Parameter None

Description Use the **default entity vad-on** command to globally configure enabling silence detection as the default value.

Use the **undo default entity vad-on** command to restore the fixed value (i.e. disabling the silence detection) to be the default value.

By default, the silence detection is disabled.

The **default entity vad-on** command is used to globally enable silence detection and make it as the default setting. After the configuration, all the voice entities and newly created voice entities on this router, which have not been configured with this function, will inherit this configuration (note that G. 711 does not support silence detection).

Related command: **vad-on**.

Example # Enable the silence detection globally.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] default entity vad-on
```

default subscriber-line

Syntax **default subscriber-line** { **receive | transmit** } **gain** *value*

undo default subscriber-line { **receive | transmit** } **gain**

View Voice view

Parameter **receive gain**: Indicates the default receive gain on all subscriber lines.

transmit gain: Indicates the default transmit gain on all subscriber lines.

Value: Value of gain on subscriber lines, in the range of -14.0 to +13.9 dB (keeps one digit after the decimal point), and defaults to 0.

Description Use the **default subscriber-line** command to configure the default receiving or transmitting gain on subscriber lines.

Use the **undo default subscriber-line** command to restore the default value.

You can use this command to increase the power of voice signal on the subscriber lines if the signal is too weak.

Related command: **transmit gain**

Example # Configure a receiving gain of 9.0 dB on all subscriber lines

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] default subscriber-line receive gain 9.0
```

delay hold

Syntax **delay hold** *milliseconds*

undo delay hold

View E&M voice subscriber line view

Parameter **hold** *milliseconds*: Specifies delay signal duration (in milliseconds) in the delay start mode. The value ranges from 100 to 5,000.

Description Use the **delay** command to configure time parameters related to the delay start mode.

Use the **delay hold** command to configure the delay signal duration in the delay start mode.

Use the **undo delay hold** command to restore the default.

By default, the delay signal duration is 400 milliseconds.

Related command: **em-signal**.

Example # Set the delay signal duration in the delay start mode to 500 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-signal delay
[Sysname-voice-line1/0] delay hold 500
```

delay rising

Syntax **delay rising** *milliseconds*

undo delay rising

View E&M voice subscriber line view

Parameter **rising** *milliseconds*: Specifies delay time (in milliseconds) from when the terminating side detects a seizure signal to when it sends a delay signal in the delay start mode. The value ranges from 20 to 2,000.

Description Use the **delay rising** command to configure a delay time from when the terminating side detects a seizure signal to when it sends a delay signal in the delay start mode.

Use the **undo delay rising** command to restore the default.

By default, the delay time is 300 milliseconds.

Related command: **em-signal**.

Example # Set the delay time from when the terminating side detects a seizure signal to when it sends a delay signal in the delay start mode to 700 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-signal delay
[Sysname-voice-line1/0] delay rising 700
```

delay send-dtmf

Syntax **delay send-dtmf** *milliseconds*

undo delay send-dtmf

View E&M voice subscriber line view

Parameter **send-dtmf** *milliseconds*: Specifies a delay (in milliseconds) before the originating side sends DTMF signals in the immediate start mode. The value ranges from 50 to 5,000.

Description Use the **delay send-dtmf** command to configure a delay before the originating side sends DTMF signals in the immediate start mode.

Use the **undo delay send-dtmf** command to restore the default.

By default, the delay before the originating side sends DTMF signals in the immediate start mode is 300 milliseconds.

Related command: **em-signal**.

Example # Set the delay before the originating side sends DTMF signals in the immediate start mode to 3,000 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1] delay send-dtmf 3000
```

delay send-wink

Syntax **delay send-wink** *milliseconds*

undo delay send-wink

View E&M voice subscriber line view

Parameter **send-wink** *milliseconds*: Specifies an interval (in milliseconds) from when the terminating side receives a seizure signal to when it sends a wink signal in the wink start mode. The value ranges from 100 to 5,000.

Description Use the **delay send-wink** command to configure an interval from when the terminating side receives a seizure signal to when it sends a wink signal in the wink start mode.

Use the **undo delay send-wink** command to restore the default.

By default, the interval from when the terminating side receives a seizure signal to when it sends a wink signal is 200 milliseconds in the wink start mode.

Related command: **em-signal**.

Example # Set the interval from when the terminating side receives a seizure signal to when it sends a wink signal in the wink start mode to 700 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
```

```
[Sysname-voice-line1/0] em-signal wink
[Sysname-voice-line1/0] delay send-wink 700
```

delay wink-hold

Syntax **delay wink-hold** *milliseconds*

undo delay wink-hold

View E&M voice subscriber line view

Parameter **wink-hold** *milliseconds*: Specifies duration (in milliseconds) the terminating side sends wink signals in the wink start mode. The value ranges from 100 to 3,000.

Description Use the **delay wink-hold** command to configure duration the terminating side sends wink signals in the wink start mode.

Use the **undo delay wink-hold** command to restore the default.

By default, the duration the terminating side sends wink signals is 500 milliseconds in the wink start mode.

Related command: **em-signal**.

Example # Set the duration the terminating side sends wink signals in the wink start mode to 700 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-signal wink
[Sysname-voice-line1/0] delay wink-hold 700
```

delay wink-rising

Syntax **delay wink-rising** *milliseconds*

undo delay wink-rising

View E&M voice subscriber line view

Parameter **wink-rising** *milliseconds*: Specifies the maximum amount of time (in milliseconds) the originating side waits for a wink signal after sending a seizure signal in the wink start mode. The value ranges from 100 to 5,000.

Description Use the **delay wink-rising** command to configure a maximum amount of time the originating side waits for a wink signal after sending a seizure signal in the wink start mode.

Use the **undo delay wink-rising** command to restore the default.

By default, the maximum amount of time the originating side waits for a wink signal after sending a seizure signal is 3,000 milliseconds in the wink start mode.

Related command: **em-signal**.

Example # Set the maximum amount of time the originating side waits for a wink signal after sending a seizure signal in the wink start mode to 2,000 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-signal wink
[Sysname-voice-line1/0] delay wink-rising 2000
```

delay start-dial

Syntax **delay start-dial** *seconds*

undo delay start-dial

View FXS/FXO voice subscriber line view

Parameter *seconds*: Dial delay in seconds, in the range of 0 to 10.

Description Use the **delay start-dial** command to configure the dial delay.

Use the **undo delay start-dial** command to restore the default.

By default, the dial delay is 1 second.

Example # Set the dial delay on FXS subscriber line 1/0 to 5 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] delay start-dial 5
```

description (voice entity view)

Syntax **description** *text*

undo description

View POTS/VoIP/VoFR entity view

Parameter *text*: Voice entity description string, consisting of up to 80 characters.

Description Use the **description** command to configure a voice entity description string.

Use the **undo description** command to delete the voice entity description string.

By default, no description is configured for the voice entity.

You can use the **description** command to add a description to a voice entity, which has no effect on the performance of the voice entity interface. You can view this description with the **display** command.

Example # Add the description local-entity 10 to voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] description local-entity10
```

description (voice subscriber line view)

Syntax **description** *text*

undo description

View FXS/FXO/E&M voice subscriber line view

Parameter *text*: Description string of voice subscriber line, consisting of up to 80 characters.

Description Use the **description** command to configure a subscriber line description string.

Use the **undo description** command to delete the description.

By default, no description is configured for the voice subscriber line.

You can use the **description** command to add a description to a voice subscriber line, which has no effect on the performance of the voice entity. You can view this description with the **display** command.

Example # Mark voice subscriber line 1/0 as lab_1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] description lab_1
```

dial-program

Syntax **dial-program**

View Voice view

Parameter None

Description Use the **dial-program** command to enter the voice dial program view.

Example # Enter the dial program view

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
```

display voice call-info

Syntax **display voice call-info** { **brief** | **mark** *tag* | **verbose** }

View Any view

Parameter **brief**: Displays the brief information of the call information table.

mark TAG: Displays the call information of the call information table by tag (in the range of 0 to 127).

verbose: Displays the detailed information of the call information table.

Description Use the **display voice call-info** command to display the contents in the call information table.

Example # Display the brief information of the call information table at a certain point of time.

```
<Sysname> display voice call-info brief
  The information table for current calls in brief
  #
  ***************** CALL 0 ***************
    ViIfIndex    : 2884067
    Module ID    : LGS  CMC
  #
  End
```

Display the detailed information of the call information table at a certain point of time.

```
<Sysname> display voice call-info verbose
  The information table for current calls in detail
  #
  ***************** CALL 0 ***************
    Call direction      : From PSTN
    ViIfIndex           : 2884067
    Related module ==>
      Module ID         : LGS
      Reference Numbers : 2
      Module ID         : CMC
      Reference Numbers : 1
    Current used voice entity : 2961
    Voice entities are offered :            2961
  #
  End
```

Table 675 Description on fields of the display voice call-info command

Field	Description
VilfIndex	Index of the voice interface from which the call is originated
Module ID	ID of a voice module that the call passes through
Call direction	Call direction of the call
Reference Numbers	Number of times of referencing the call information table of a call
entity	Voice entity involved in the call.

display voice cmc

Syntax **display voice cmc** { **ccb | statistic** [**all | em | h323 | iva | lgs | r2 | sip | tmrout | vim**] }

View Any view

Parameter **ccb**: Displays the call control block of CMC module

statistic: Displays statistics information related to CMC module.

all: Displays all statistics information related to CMC module.

em: Displays EM module information related to CMC module.

h323: Displays H.323 module information related to CMC module.

iva: Displays IVA module information related to CMC module.

lgs: Displays relevant LGS module information related to CMC module.

r2: Displays R2 module information related to CMC module.

sip: Displays SIP module information related to CMC module.

tmrout: Displays timeout information of the timer in CMC module.

vim: Displays VIM module information related to CMC module.

Description Use the **display voice cmc** command to display messages which are related to CMC module. These messages mainly contain call control block messages and statistic messages, in which statistic messages can be classified and displayed according to the type of messages and the interaction with surrounding modules.

Example # Display the information of the call control block of CMC module.

```
<Sysname> display voice cmc ccb
 The CMC Module Call Control Block Information!
 #
 *************** CCB[1] ***************
   GblCallID        : 0x10000
   CalledAddr       : 2961
   CalledAddrSubst  : 2961
```

```
   CallerAddr       :
   CallerAddrSubst  :
   CallInfoTabIndex : 0
   Call Leg Number  : 2
...Active Service   : 0
   INCOMING CALLLEG NUMBER : 1
    INCOMING LEG[0]
    {
      Spl Protocol  : LGS
      LocalRef      : 0x0002
      IfIndex       : 2884067
      IpAddress     : 0.0.0.0
      IpPort        : 0
      LegState      : IN_STATE_ACTIVE
      ConnectState  : CONN_STATE_ACTIVE
    }

   OUTGOING CALLLEG NUMBER : 1
    OUTGOING LEG[0]
    {
      Spl Protocol  : LGS
      LocalRef      : 0x0003
      IfIndex       : 2884064
      IpAddress     : 0.0.0.0
      IpPort        : 0
      LegState      : OUT_STATE_ACTIVE
      ConnectState  : CONN_STATE_ACTIVE
    }
 #
 End.
```

Display LGS statistics information related to the CMC module

```
<Sysname>display voice cmc statistic lgs
  ACCP Message statistics between CMC and LGS:
  {
    Send SETUP message            :  0
    Send SETUP_ACK message        : 0
    Send ALERTING message         :  0
    Send CONNECT message          : 0
    Send RELEASE message          :  0
    Send RELEASE_COMP message     : 0
    Send INFORMATION message      :  0
    Send SWITCH_CODEC message     : 0
    Send FAXVOC_SWTH message      :  0
    Send FAXVOC_SWTHACK message   : 0

    Receive SETUP message         :  0
    Receive SETUP_ACK message     : 0
    Receive ALERTING message      :  0
    Receive CONNECT message       : 0
    Receive RELEASE message       :  0
    Receive RELEASE_COMP message  : 0
    Receive INFORMATION message   :  0
    Receive SWITCH_CODEC message  : 0
    Receive FAXVOC_SWTH message   :  0
    Receive FAXVOC_SWTHACK message: 0
  }
```

Table 676 Description on fields of the display voice cmc command

Field	Description
GblCallID	Indicates the global ID of the call.
CalledAddr	Indicates the called number of the call.
CalledAddrSubst	Indicates the called number after substitution
CallerAddr	Indicates the caller number of the call.
CallerAddrSubst	Indicates the caller number after substitution
CallInfoTabIndex	Indicates the call information index of the call.
Call Leg Number	Indicates the number of call legs of the call
Active Service	Indicates the number of services involved in the call
Spl Protocol	Indicates the type of protocol used in the call leg
LocalRef	Indicates the local call identifier of the call leg.
IfIndex	Indicates the voice interface index connected to the call leg
IpAddress	Indicates the IP address connected to the call leg
IpPort	Indicates the port number connected to the call leg
LegState	Indicates the state of the call leg
ConnectState	Indicates the state of connection of the call
SETUP message	Statistics of SETUP message
SETUP_ACK message	Statistics of SETUP_ACK message
ALERTING message	Statistics of ALERTING message
CONNECT message	Statistics of CONNECT message
RELEASE message	Statistics of RELEASE message
RELEASE_COMP message	Statistics of RELEASE_COMP message
INFORMATION message	Statistics of INFORMATION message
SWITCH_CODEC message	Statistics of SWITCH_CODEC message
FAXVOC_SWTH message	Statistics of FAXVOC_SWTH message
FAXVOC_SWTHACK message	Statistics of FAXVOC_SWTHACK message

display voice default all

Syntax **display voice default all**

View Any view

Parameter None

Description Use the **display voice default all** command to view the current default values and the system-fixed default values for voice and fax. For example, truncated called number is used according to the default settings and system-fixed default settings.

For example, the carrier transmission energy level of GW defaults to 10 (the system-fixed default value is 15).

Example # Display the current default values and the system-default values.

```
<Sysname> display voice default all
    default entity fax ecm off(system: off)
    default entity fax protocol t38(system: t38)
    default entity fax protocol t38 hb-redundancy 0(system: 0)
    default entity fax protocol t38 lb-redundancy 0(system: 0)
    default entity fax level 15(system: 15)
    default entity fax local-train threshold 10(system: 10)
    default entity fax baudrate voice(system: voice)
    default entity fax nsf-on off(system: off)
    default entity fax train-mode ppp(system: ppp)
    default entity compression 1st-level g729r8(system: g729r8)
    default entity compression 2nd-level g711alaw(system: g711alaw)
    default entity compression 3rd-level g711ulaw(system: g711ulaw)
    default entity compression 4th-level g723r53(system: g723r53)
    default entity vad-on off(system: off)
    default entity payload-size g711    20(system: 20)
    default entity payload-size g723    30(system: 30)
    default entity payload-size g726r16 30(system: 30)
    default entity payload-size g726r24 30(system: 30)
    default entity payload-size g726r32 30(system: 30)
    default entity payload-size g726r40 30(system: 30)
    default entity payload-size g729    30(system: 30)
```

Table 677 Description on fields of the display voice default command

Field	Description
fax ecm	ECM mode is used for Fax
fax protocol t38	Fax protocol for intercommunication
fax redundancy t38 hb-redundancy	Number of high-speed redundant packets, available for standard T.38 or T.38
fax redundancy t38 lb-redundancy	Number of low-speed redundant packets, available for standard T.38 or T.38
fax level	Gateway carrier transmitting energy level
fax local-train threshold	Fax local training threshold percentage
fax baudrate	Highest Fax rate
fax nsf-on	Fax capacity negotiation mode
fax train-mode	Fax training mode
compression 1st-level	Voice coding mode of the first preference
compression 2nd-level	Voice coding mode of the second preference
compression 3rd-level	Voice coding mode of the third preference
compression 4th-level	Voice coding mode of the fourth preference
vad-on	Voice entity VAD
payload-size g711	Voice entity packet assembly interval (G.711)
payload-size g723	Voice entity packet assembly interval (G.723)
payload-size g726r16	Voice entity packet assembly interval (G.723 r16)
payload-size g726r24	Voice entity packet assembly interval (G.723 r24)
payload-size g726r32	Voice entity packet assembly interval (G.723 r32)
payload-size g726r40	Voice entity packet assembly interval (G.723 r40)
payload-size g729	Voice entity packet assembly interval (G.729)

display voice entity

Syntax **display voice entity** { **all** | **mark** *entity-tag* | **pots** | **voip** }

View Any view

Parameter **all**: Displays all voice entities.

pots: Displays all POTS entities.

mark *entity-tag*: Displays the voice entity specified by a tag (in the range of 1 to 2147483647).

voip: Displays all VoIP entities.

Description Use the **display voice entity** command to view the configuration information of voice entities.

Normally speaking, you can use the **display current-configuration** command to view the information of all the active interfaces in the router as well as the global configuration information. But it will display a great deal of information. So if you just want to view the configuration information of voice entities, you can use the **display voice entity** command.

Example # Display the configuration information of POTS voice entities.

```
<Sysname> display voice entity all
 Current configuration of entities
 !
 entity 66 pots
  match-template 6600..
  line 6/0
 !
End
```

Table 678 Description on fields of the display voice entity command

Field	Description
Current configuration of entities	Configured voice entities
entity 66 pots	POTS entity numbered 66
match-template	Template for number matching
line	Voice subscriber line bound to the voice entity

display voice ipp statistic

Syntax **display voice ipp statistic** { **all** | **cmc** | **h225** | **h245** | **ras** | **socket** | **timer** }

View Any view

Parameter **all**: Displays all statistics about the IPP module.

cmc: Displays statistics about CMC.

h225: Displays statistics about H.225 messages.

h245: Displays statistics about H.245 messages.

ras: Displays statistics about ras messages.

socket: Displays statistics about socket messages.

timer: Displays timeout statistics.

Description Use the **display voice ipp** command to display statistics about the IPP module.

Example # Display statistics about H.225 messages of the IPP module.

```
<Sysname> display voice ipp statistic h225
  Statistics about H225 :
  {
    Send_Setup                    :  0
    Send_CallProceeding           :  0
    Send_Alerting                 :  0
    Send_Connect                  :  0
    Send_ReleaseComplete          :  0
    Send_FacilityIndUserInput     :  0
    Send_FacilityTCSRequest       :  0
    Send_FacilityTCSAck           :  0
    Send_FacilityTCSReject        :  0
    Send_FacilityOLCRequest       :  0
    Send_FacilityOLCAck           :  0
    Send_FacilityOLCReject        :  0
    Send_FacilityMSDRequest       :  0
    Send_FacilityMSDAck           :  0
    Send_FacilityMSDReject        :  0
    Send_FacilityCLCRequest       :  0
    Send_FacilityCLCAck           :  0
    Send_FacilityStartH245        :  0
    Send_Error                    :  0
    Recv_Setup                    :  0
    Recv_CallProceeding           :  0
    Recv_Alerting                 :  0
    Recv_Connect                  :  0
    Recv_ReleaseComplete          :  0
    Recv_Progress                 :  0
    Recv_FacilityTCSRequest       :  0
    Recv_FacilityTCSAck           :  0
    Recv_FacilityTCSReject        :  0
    Recv_FacilityOLCRequest       :  0
    Recv_FacilityOLCAck           :  0
    Recv_FacilityOLCReject        :  0
    Recv_FacilityMSDRequest       :  0
    Recv_FacilityMSDAck           :  0
    Recv_FacilityMSDReject        :  0
    Recv_FacilityCLCRequest       :  0
    Recv_FacilityCLCAck           :  0
    Recv_Unknown                   :  0
  }
```

Table 679 Description on fields of the display voice ipp statistic command

Field	Description
Setup	Statistics of Setup messages
CallProceeding	Statistics of CallProceeding messages
Alerting	Statistics of Alerting messages
Connect	Statistics of Connect messages
ReleaseComplete	Statistics of ReleaseComplete messages
FacilityIndUserInput	Statistics of UserInput messages
FacilityTCSRequest	Statistics of TCS Request messages
FacilityTCSAck	Statistics of TCS Acknowledgement messages
FacilityTCSReject	Statistics of TCS Reject messages
FacilityOLCRequest	Statistics of OLC Request messages
FacilityOLCAck	Statistics of OLC Acknowledgement messages
FacilityOLCReject	Statistics of OLC Reject messages
FacilityMSDRequest	Statistics of MSD Request messages
FacilityMSDAck	Statistics of MSD Acknowledgement messages
FacilityMSDReject	Statistics of MSD Reject messages
FacilityCLCRequest	Statistics of CLC Request messages
FacilityCLCAck	Statistics of CLC Acknowledgement messages
FacilityStartH245	Statistics of H245 Start messages
Error	Statistics of H245 Error messages
Unknown	Statistics of H245 Unknown messages

display voice iva statistic

Syntax **display voice iva statistic** { **all** | **call** | **cmc** | **error** | **isdn** | **proc** | **timer** | **vim** }

View Any view

Parameter **all**: Displays all the statistic information related to IVA module.

call: Displays the calling statistics in the IVA module.

cmc: Displays all the interaction statistics between IVA module and CMC.

error: Displays all the error statistics of IVA module.

isdn: Displays the interaction statistics between IVA module and ISDN.

proc: Displays the statistic information of process call in IVA module.

timer: Displays the timer's statistic information of IVA module.

vim: Displays all the interaction statistic information between IVA module and VIM.

Description Use the **display voice iva statistic** command to view the call statistics between IVA module and other modules.

The command can display information such as the total number of call message, number of successful call message, number of failed call message of ISDN, CMC and VIM in IVA module. You can also use the keywords (such as **isdn**, **cmc**) to display the statistics of the corresponding modules.

Example # Display the call statistics between IVA module and other modules.

```
<Sysname> display voice iva statistic call
Statistics about IVA calls :
    {
      IVA_ISDN_ACTIVE_CALL                  :  0
      IVA_ISDN_ACTIVE_CALL_SUCCEEDED        :  0
      IVA_ISDN_ACTIVE_CALL_FAILED           :  0
      IVA_ISDN_PASSIVE_CALL                 :  0
      IVA_ISDN_PASSIVE_CALL_SUCCEEDED       :  0
      IVA_ISDN_PASSIVE_CALL_FAILED          :  0
    }
```

Table 680 Description on fields of the display voice iva statistic command

Field	Description
IVA_ISDN_ACTIVE_CALL	Statistics of calls generated when IVA serves as the caller
IVA_ISDN_ACTIVE_CALL_SUCCEEDED	Statistics of successful calls when IVA serves as the caller
IVA_ISDN_ACTIVE_CALL_FAILED	Statistics of failed calls when IVA serves as the caller
IVA_ISDN_PASSIVE_CALL	Statistics of calls generated when IVA serves as the called
IVA_ISDN_PASSIVE_CALL_SUCCEEDED	Statistics of successful calls when IVA serves as the called
IVA_ISDN_PASSIVE_CALL_FAILED	Statistics of failed calls when IVA serves as the called

display voice subscriber-line

Syntax **display voice subscriber-line** *line-number*

View Any view

Parameter *line-number*: Subscriber line number.

Description Use the **display voice subscriber-line** command to view the configuration information of the subscriber line, such as the type, status, codec mode, receive and transmit gain, and so on.

Related command: **subscriber-line**.

Example # Display the configuration information about E&M voice subscriber line 5/0.

```
<Sysname> display voice subscriber-line 5/0
  Current information  -----  subscriber-line5/0
    Type                         = Analog E&M Immediate-Start
    Status                       = UP
Call Status                  = BUSYTONE
...Description                  = subscriber-line5/0 Interface
    Private Line                 = None
    Cng                          = Enable
    Echo Canceller               = Enable
    Echo Canceller Tail-Length   = 32
    Nlp On                       = Enable
    Fax Detect Mode              = CNG/CED
    Ring Generate                = Enable
    Receive Gain                 = 0.0
    Transmit Gain                = 0.0
    DTMF Threshold Analogue :
        Index  0                 = 1400
        Index  1                 = 458
        Index  2                 = -9
        Index  3                 = -9
        Index  4                 = -9
        Index  5                 = -9
        Index  6                 = -3
        Index  7                 = -12
        Index  8                 = -12
        Index  9                 = 30
        Index 10                 = 300
        Index 11                 = 3200
        Index 12                 = 375
    Timer Dial-Interval          = 10
    Timer Wait-Digit             = 5
    Timer Ring-Back              = 60
    Delay Send-dtmf              = 300
    E&M Physical Wire            = 4-Wire
    E&M Type                     = V
    Slic-Gain                    = 0.8 db
    Physical Information :
        Card Type                = E&M
        Physical State           = 1
        Logical State            = 1
        Voice State              = Uninstall
        ResetCount               = 0
        InPkts                   = 0
        OutPkts                  = 0
        InBytes                  = 0
        OutBytes                 = 0
        LastRcvPacketLen         = 0
        LastSndPacketLen         = 0
        CmdInBuff                = 0
        CmdInTotalBuff           = 0
        DataInBuff               = 0
        DataInTotalBuff          = 0
        AbortCmdCount            = 0
        AbortPktsCount           = 0
        G723R53ToR63Packet       = 0
        G723R63ToR53Packet       = 0
        ClearDspBuffCount        = 0
```

Table 681 Description on fields of the display voice subscriber-line command

Field	Description
Type	Type of voice subscriber line
Status	Status of voice subscriber line
Call Status	Call status of voice subscriber line
Description	Description of voice subscriber line
Private-line	Private line dial number of voice subscriber line
CNG	Comfortable noise configuration on voice subscriber line
EchoCancel	Echo duration configuration on voice subscriber line
Nlp-on	Non-linear process of echo cancel on voice subscriber line
Fax detect mode	Fax detection mode configuration on voice subscriber line
Ring generate	Ring generation configuration on voice subscriber line
Receive gain	Receive gain configuration on voice subscriber line
Transmit gain	Transmit gain configuration on voice subscriber line
DTMF Threshold Analogue	DTMF threshold configuration of analog voice subscriber line
Timer Dial-Interval	Dial interval of voice subscriber line
Timer Wait-Digit	Period of timeout waiting for a number on voice subscriber line
Timer Ring-Back	Period of timeout when ringing back on voice subscriber line
Delay Send-dtmf	Pre-dial delay of voice subscriber line
E&M Physical Wire	Cable type of analog E&M voice interface
E&M Type	Circuit type of analog E&M voice interface
Slic-Gain	SLIC gain configuration of analog E&M voice interface
Physical Information	Physical statistics information
Card Type	Type of the voice interface card
Physical State	Physical state of the voice interface
Logical State	Logical state of the voice interface
Voice State	Call state on the voice interface
ResetCount	Indicates how many times the voice interface card is reset
InPkts	Number of received packets on the voice interface
OutPkts	Number of sent packets on the voice interface
InBytes	Bytes of received packets on the voice interface
OutBytes	Bytes of sent packets on the voice interface
LastRcvPacketLen	Length of the last received packet on the voice interface
LastSndPacketLen	Length of the last sent packet on the voice interface
CmdInBuff	Number of commands in the command buffer of the voice interface
CmdInTotalBuff	Total number of commands in the command buffers of the voice interface card
AbortCmdCount	Number of command packets discarded on the voice interface
AbortPktsCount	Number of packets discarded on the voice interface
G723R53ToR63Packet	Number of G723R53 packets converted to G723R63 packets on the voice interface
G723R63ToR53Packet	Number of G723R63 packets converted to G723R53 packets on the voice interface
ClearDspBuffCount	Number of DSP buffers cleared on the voice interface

dscp media

Syntax **dscp media** *dscp-value*

undo dscp media

View POTS/VoIP entity view

Parameter *dscp-value*: DSCP value in the range of 0 to 63 or the keyword **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, and **ef**.

Description Use the **dscp media** command to set the DSCP value in the ToS field in the IP packets that carry the RTP stream of the voice entity.

Use the **undo dscp media** command to restore the default DSCP.

By default, the DSCP value is ef (101110).

Example # Set the DSCP value in the ToS field of the IP packets that carry the RTP stream of VoIP voice entity to af41.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 2 voip
[Sysname-voice-dial-entity2] dscp media af41
```

dtmf amplitude

Syntax **dtmf amplitude** *value*

undo dtmf amplitude

View Voice view

Parameter *value:* DTMF amplitude in 0.1 dBm increments, in the range of -9.0 to -7.0.

Description Use the **dtmf amplitude** command to configure the DTMF amplitude. Once configured, the parameter applies to the whole device.

Use the **undodtmf amplitude** command to restore the default value.

By default, the DTMF amplitude is -9.0 dBm.

Note that the configuration will apply to the whole device once you carry out this command.

Example # Configure the DTMF amplitude to -8.0 dBm

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dtmf amplitude -8.0
```

dtmf sensitivity-level

Syntax **dtmf sensitivity-level** { **high** | **low** }

undo dtmf sensitivity-level

View Analog FXS/FXO voice subscriber line view

Parameter **high**: Sets the DTMF detection sensitivity high. In this mode, the reliability is low and detection errors may occur.

low: Sets the DTMF detection sensitivity low. In this mode, the reliability is high, but DTMF undetection may occur.

Description Use the **dtmf sensitivity-level** command to set the DTMF detection sensitivity level.

Use the **undo dtmf sensitivity-level** command to restore the default detection sensitivity level.

By default, the DTMF detection sensitivity level is high.

This command is valid only for FXS/FXO interfaces.

Example # Set the DTMF detection sensitivity level of voice subscriber line 1/0 to low.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] dtmf sensitivity-level low
```

dtmf time

Syntax **dtmf time** { **interval | persist** } *milliseconds*

undo dtmf time { **interval | persist** }

View Voice view

Parameter **persist:** Specifies the persisting time of sending DTMF.

Interval: Specifies the interval for sending DTMF.

milliseconds: Time in milliseconds, in the range of 50 to 500.

Description Use the **dtmf time** command to configure the related time parameters of DTMF.

Use the **undo dtmf time** command to restore the default.

By default, the persisting time of sending DTMF and the interval for sending DTMF are both 120 milliseconds.

Note that the configuration will apply to the whole interface once you carry out the command.

Example # Set the persisting time of sending DTMF digits to 200 milliseconds, and the interval to 300 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dtmf time persist 200
[Sysname-voice] dtmf time interval 300
```

dtmf threshold

Syntax **dtmf threshold analog** *index value1*

undo dtmf threshold analog *index*

View Analog FXS/FXO/E&M voice subscriber line view

Parameter **analog**: Analog voice subscriber line.

index: Index number corresponding to a threshold, an integer in the range of 0 to 12.

value: Threshold corresponding to the specified index. The value range varies with indexes. For details, see Table 682.

According to the energy level of the row and column frequencies as well as the energy level of their double frequencies, the system determines whether the input DTMF digit is valid.

The maximum energy of the input signal in the row frequency group is ROWMAX and the corresponding double frequency energy is ROW2nd. The maximum energy in the column frequency group is COLMAX and the corresponding double frequency energy is COL2nd.

Table 682 Meaning of the index numbers

Index	Meaning	Value range	Remarks
0	The lower limit of (ROWMAX + COLMAX). The input signal which is otherwise regarded too weak is recognized as a DTMF digit when ROWMAX + COLMAX) > 0.	1 to 4,999, with a default of 1,400	The larger the value is, the higher the detection reliability is. However, the sensitivity drops.

Table 682 Meaning of the index numbers

Index	Meaning	Value range	Remarks
1	The upper limit of the maximum value of ROWMAX or COLMAX, whichever is larger. This limit is used for detecting the inter-digit delay. A detected digit is regarded ended only when max (ROWMAX, COLMAX) < 1.	1 to 4,999, with a default of 458	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
2	The lower limit of COLMAX/ROWMAX, where ROWMAX < COLMAX. An input signal is recognized as a DTMF digit only when 10 x (COLMAX/ROWMAX) > 2.	-18 to -3 dB, with a default of -9 dB.	The larger the value is, the higher the detection reliability is. However, the sensitivity drops.
3	The lower limit of ROWMAX/COLMAX when COLMAX Š ROWMAX. The function is similar to that of index 2. An input signal is recognized as a DTMF digit only when 10 x (ROWMAX/COLMAX) > 2.	-18 to -3 dB, with a default of -9 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
4	The upper limit of the ratio of the second largest energy level from the row frequency group to ROWMAX. The ratio must be lower than this limit for the input signal to be recognized as a DTMF digit.	-18 to -3 dB, with a default of -9 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
5	The upper limit of the ratio of the second largest energy level from the column frequency group to COLMAX. The ratio must be lower than this limit for the input signal to be recognized as a DTMF digit.	-18 to -3 dB, with a default of -9 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
6	The upper limit of ROW2nd/ROWMAX. An input signal is recognized as a DTMF digit only when ROW2nd/ROWMAX < 6.	-18 to -3 dB, with a default of -3 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
7	The upper limit of COL2nd/COLMAX. The ratio must be lower than this limit for the input signal to be recognized as a DTMF digit.	-18 to -3 dB, with a default of -12 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
8	The upper limit of the ratio of the maximum energy level of two extra specified frequency points to max (ROWMAX, COLMAX). The ratio must be greater than this upper limit for the input signal to be recognized as a DTMF digit.	-18 to -3 dB, with a default of -12 dB.	The smaller the value is, the higher the detection reliability is. However, the sensitivity drops.
9	The lower limit of the DTMF signal duration. The duration of DTMF key tone must be larger than this threshold for the input signal to be recognized as a DTMF digit.	30 to 150 milliseconds, with a default of 30 milliseconds.	The larger the value is, the higher the detection reliability is. However, the sensitivity drops.

Table 682 Meaning of the index numbers

Index	Meaning	Value range	Remarks
10	The frequency of the first extra frequency point specified for detection. In addition, it must be a frequency 100 Hz greater than or less than the row and column frequency groups.	300 to 3,400 Hz, with a default of 300 Hz.	-
11	The frequency of the second extra frequency point specified for detection. In addition, it must be a frequency 100 Hz greater than or less than the row and column frequency groups.	300 to 3,400 Hz, with a default of 3,200 Hz.	-
12	The lower limit of the amplitude of the input signal. The average amplitude must be greater than this threshold for the input signal to be recognized as a DTMF digit.	0 to 700, with a default of 375.	The larger the value is, the higher the detection reliability is. However, the sensitivity drops.

Description Use the **dtmf threshold** command to configure the sensitivity of DTMF digit detection.

Use the **undo dtmf threshold** command to restore the default.

The **dtmf threshold** command issues the thresholds for DTMF dial tone detection to the underlying layer DSP for the purpose of tuning detection sensitivity and reliability of the device subtly. Inside the DSP, a set of generic default values have been configured. They are 1,400, 458, -9, -9, -9, -9, -3, -12, -12, 30, 300, 3,200, 375, with their index being 0 through 12. Professionals can use this command to adjust the device when DTMF digit detection fails. In normal cases, the defaults are adopted.

Example # Set DTMF threshold 9 in voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] dtmf threshold analog 9 40
```

echo-canceller

Syntax **echo-canceller** { **enable** | **tail-length** *milliseconds* }

undo echo-canceller { **enable** | **tail-length** }

View FXS/FXO/E&M voice subscriber line view

Parameter **enable**: Enables the echo cancellation (EC) function.

tail-length *milliseconds*: Echo duration in milliseconds, that is, the time that elapses from when a subscriber speaks to when he hears the echo. It ranges from 0 to 64, with a default of 32.

Description Use the **echo-canceller** command to enable echo cancellation and set the echo duration.

Use the **undo echo-canceller** command to disable the EC function.

By default, the EC function is disabled.

*This command is applicable only after the **echo-canceller enable** command is executed.*

Related command: **subscriber-line** and **echo-canceller parameter**.

Example Configure the echo duration on voice subscriber line 1/0 to 24 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-dial-line1/0] echo-canceller enable
[Sysname-voice-dial-line1/0] echo-canceller tail-length 24
```

echo-canceller parameter

Syntax **echo-canceller parameter** { **convergence-rate** *value* | **max-amplitude** *value* | **mix-proportion-ratio** *value* | **talk-threshold** *value* }

undo echo-canceller parameter { **convergence-rate | max-amplitude | mix-proportion-ratio | talk-threshold** }

View Voice view

Parameter **convergence-rate** *value*: Sets the convergence rate of comfort noise amplitude. It ranges from 0 to 511. The greater the value, the quicker the convergence.

max-amplitude *value*: Sets the maximum amplitude of comfort noise. It ranges from 0 to 2,048. The higher the value, the greater the maximum noise amplitude. The value "0" indicates that the system performs only nonlinear processing and does not add comfort noise.

mix-proportion-ratio *value*: Sets the comfort noise mixture proportion control factor. It ranges from 0 to 3,000 and defaults to 100. The greater the value, the higher the proportion of noise in the hybrid of noise and voice.

talk-threshold *value*: Sets the threshold of two-way talk. It ranges from 0 to 2.

Description Use the **echo-canceller parameter** command to configure echo cancellation parameters.

Use the **undo echo-canceller** command to restore the default.

By default, the convergence rate of comfort noise amplitude is 0, the maximum amplitude of comfort noise is 256, the comfort noise mixture proportion control factor is 100, and the threshold of two-way talk is 1.

Related command: **echo-canceller**.

Example # Set the convergence rate of comfort noise amplitude to 50.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] echo-canceller parameter convergence-rate 50
```

em-phy-parm

Syntax **em-phy-parm** { **2-wire** | **4-wire** }

undo em-phy-parm

View Analog E&M voice subscriber line view

Parameter **2-wire**: Chooses the 2-wire analog E&M wire scheme.

4-wire: Chooses the 4-wire analog E&M wire scheme.

Description Use the **em-phy-parm** command to configure a wire scheme for the analog E&M subscriber line.

Use the **undo em-phy-parm** command to restore the default.

By default, the 4-wire analog E&M cable is selected.

This command is only applicable only to the analog E&M subscriber line. The configuration will apply to all E&M interfaces of the card after you configure this command.

Example # Choose the 4-wire scheme for the analog E&M subscriber line.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-phy-parm 4-wire
```

em-signal

Syntax **em-signal** { **delay** | **immediate** | **wink** }

undo em-signal

View E&M voice subscriber line view

Parameter **delay**: When using the delay start mode, the calling end occupies the trunk line, and the called end, such as PBX, will also enter the hook-off state to respond the caller till it is ready for receiving the called number.

immediate: Immediate start mode. The caller end hooks off to seize the line through line E and sends the called number. The prerequisite for using the immediate start mode is: The equipment at the remote end should listen to the dial signal immediately after identifying the off-hook signal.

wink: Wink start mode. The caller end hooks off to seize the line through line E, and it has to wait for a wink signal from the remote end before sending out the called number.

Description Use the **em-signal** command to configure a start mode for an analog E&M voice subscriber line.

Use the **undo em-signal** command to restore the default start mode.

By default, the immediate start mode is selected for the analog E&M subscriber line.

Related command: delay.

Example # Configure delay mode.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] em-signal delay
```

entity

Syntax **entity** *entity-number* { **pots** | **voip** }

undo entity { *entity-number* | **all** | **pots** | **voip** }

View Voice dial program view

Parameter *entity-number*: Identifies a voice entity. The value ranges from 1 to 2147483647.

all: All voice entities.

pots: Indicates that the voice entity originates a call from the local voice subscriber line.

voip: Indicates that the voice entity originates a call from the network side.

Description Use the **entity** command to enter voice entity view, or configure a voice entity and then enter its view if the voice entity does not exist.

Use the **undo entity** command to remove the existing voice entity.

In a global view, use the **entity** command to enter a voice entity view, and use **quit** to return to the dial program view.

The entity-number assigned to a VoIP or POTS entity must be unique among all VoIP and POTS entities.

Related command: **line**.

Example # Create and enter the voice entity view to configure a POTS voice entity whose identification is 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
```

fast-connect

Syntax **fast-connect**

undo fast-connect

View VoIP entity view

Parameter None

Description Use the **fast-connect** command to enable fast connection for H.323 calls.

Use the **undo fast-connect** command to disable fast connection.

By default, fast connection is disabled.

As there is no ability negotiation for fast connection mode, the ability confirmation of the two parties is determined by the called gateway. When the router acts as an originating gateway, you can set whether or not to apply fast connection mode for each originated call. When the router acts as a terminating gateway, the configuration of the **voip called-start** command will determine whether fast connection is used for call initialization.

Fast connection procedure will be used when both the calling and called parties support fast connection. Provided that neither the calling nor the called gateway supports fast connection mode, the system will automatically switch to normal connect procedure to resume the call.

It is OK to only configure **fast-connect** command for VoIP voice entity on the calling gateway. Just after successfully enabling fast connection can the tunnel function be configured.

Related command: **outband**, **tunnel-on**, and **voip called-start**.

Example # Enable fast connection for VoIP voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] fast-connect
```

hookoff-mode

Syntax **hookoff-mode** { **delay** | **immediate** }

undo hookoff-mode

View Analog FXO voice subscriber line view

Parameter **delay:** Specifies the FXO voice subscriber line to operate in the delay off-hook mode.

immediate: Specifies the FXO voice subscriber line to operate in the immediate off-hook mode.

Description Use the **hookoff-mode** command to configure the off-hook mode for the FXO voice subscriber line.

Use the **undo hookoff-mode** command to restore the default.

By default, the FXO voice subscriber line operates in the immediate off-hook mode.

Example # Specify an FXO voice subscriber line to operate in the delay off-hook mode.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-subscriber-line 1/0] hookoff-mode delay
```

hookoff-mode delay bind

Syntax **hookoff-mode delay bind** *fxs_subscriber_line*

undo hookoff-mode delay bind

View Analog FXO voice subscriber line view

Parameter *fxs_subscriber_line*: FXS voice subscriber line bound to the FXO voice subscriber line.

Description Use the **hookoff-mode delay bind** command to bind an FXS voice subscriber line to the FXO voice subscriber line.

Use the **undo hookoff-mode** command to remove the binding.

By default, no FXS voice subscriber line is bound to the FXO voice subscriber line.

After an FXS voice subscriber line is bound to the FXO voice subscriber line, the off-hook/on-hook state of these two lines will be consistent.

- *To keep the consistent off-hook/on-hook state between the bound FXS and FXO voice subscriber lines, you must consider the configurations of the **private-line** and **caller-permit** commands when executing the **hookoff-mode delay bind** fxs_subscriber_line command. The FXS voice subscriber line specified by fxs_subscriber_line must be the one to which the dedicated line number points. In addition, only the bound FXS voice subscriber line is allowed to originate calls to the FXO voice subscriber line by restricting incoming calls.*
- *The bound FXS and FXO voice subscriber lines must come from the same device.*

Example # Specify the delay off-hook mode for the FXO voice subscriber line and bind FXS voice subscriber line 1/24 to the FXO voice subscriber line.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-subscriber-line 1/0] hookoff-mode delay bind 1/24
```

hookoff-time

Syntax **hookoff-time** *time*

undo hookoff-time

View Analog FXO voice subscriber line view

Parameter *time*: Length of the on-hook timer in seconds, in the range of 60 to 36,000.

Description Use the **hookoff-time** command to configure the on-hook timer length.

Use the **undo hookoff-time** command to restore the default on-hook timer length.

By default, no on-hook timer length is set.

Example # Set the on-hook timer length to 500 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] hookoff-time 500
```

impedance

Syntax **impedance** { *country-name* | **R550** | **R600** | **R650** | **R700** | **R750** | **R800** | **R850** | **R900** | **R950** }

undo impedance

View Analog FXO voice subscriber line view

Parameter *country-name*: Specifies a country so that its impedance standard is used. It can be Australia, Austria, Belgium-Long, Belgium-Short, Brazil, China, Czech-Republic, Denmark, ETSI-Harmanized, Finland, France, German-Swiss, Greece, Hungary, India, Italy, Japan, Korea, Mexico, Netherlands, Norway, Portugal, Slovakia, Spain, Sweden, U.K.: US-Loaded-Line, US-Non-Loaded, or US-Special-Service.

R550: 550-ohm real impedance.

R600: 600-ohm real impedance.

R650: 650-ohm real impedance.

R700: 700-ohm real impedance.

R750: 750-ohm real impedance.

R800: 800-ohm real impedance.

R850: 850-ohm real impedance.

R900: 900-ohm real impedance.

R950: 950-ohm real impedance.

Description Use the **impedance** command to configure the current electrical impedance on an FXO voice subscriber line.

Use the **undo impedance** command to restore the default.

By default, the electrical impedance on the FXO voice subscriber line applies to China.

You can specify an impedance value by specifying the country where the value applies. You may just input the leading letters that uniquely identify a country without inputting a complete country name, however.

Example # Configure the current electric impedance to **r600** on voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] impedance r600
```

line

Syntax **line** *line-number*

undo line

View POTS entity view

Parameter *line-number:* Number of a subscriber line.

Description Use the **line** command to associate the voice entity with a specified voice subscriber line.

Use the **undo line** command to remove this association.

By default, there is no association between a voice entity and a voice subscriber line.

Example # Associate voice entity 10 and voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] line 1/0
```

match-template

Syntax **match-template** *match-string*

undo match-template

View POTS/VoIP/VoFR entity view

Parameter *match-string*: Number template. Its format is [**+**] { *string* [**T**] [**$**] | **T** }, with the maximum length of 31 characters. The characters are described in the following.

- **+**: Appears at the beginning of a calling number to indicate that the number is E.164-compliant.
- **$**: Is the last character, indicating the end of the number. That means the entire called number must match the string part before "$".
- **T**: Timer. It means the system is waiting the subscriber for dialing any number till: the number length threshold is exceeded, or the subscriber inputs the terminator; or the timer expires. T is used to match a number with any digits.
- *string*: A string composed of any characters of "0123456789#*.!+%[]()-". The meanings of the characters are described in the following table:

Table 683 Meanings of the characters in string

Character	Meaning
0-9	Numbers from 0 to 9. Each means a digit.
# and *	Each means a valid digit.
.	A wildcard. It can match any digit of a valid number. For example, 555. . . . matches any string that begins with 555 and with four additional characters.
!	The character or characters right in front of it does not appear or appears once. For example, 56!1234 can match 51234 and 561234.
+	The character or characters right in front of it appears once or several times. But its appearance at the beginning of the whole number means the number is E.164-compliant. For example, (1) 9876(54)+ matches 987654, 98765454, 9876545454 and so on. (2) +110022 indicates 110022 is compliant with E.164.
-	Hyphen. It connects two values (the smaller one before it and the bigger one after it) to indicate a range. For example, "1-9" means numbers from 1 to 9 (inclusive).
%	The character or characters right in front of it does not appear, or appears several times. For example, 9876(54)% matches 9876, 987654, 98765454, 9876545454 and so on.
[ ]	Select one character from the group. For example, [1-36] can match only one character among 1, 2, 3, and 6.
( )	A group of characters. For example, (123) means a string "123". It is usually used with "!", "%", and "+". For example, "408(12)+" can match 40812 or 408121212. But it cannot match 408. That is, "12" can appear continuously and it must at least appear once.

- *The character or characters in front of "!", "%", and "+" are not to be matched accurately. They are handled similar to the wildcard ".". Moreover, these symbols cannot be used alone. There must be a valid digit or digits in front of them.*
- *If you want to use "[ ]" and "( )" at the same time, you must use them in the format "([ ])". Other formats, such as "[[ ]]" and "[( )]" are illegal.*
- *"-" can only be used in "[ ]", and it only connects the same type of characters, such as "0-9". The formats like "0-A" are illegal.*

Description Use the **match-template** command to configure the number template for a voice entity.

Use the **undo match-template** command to remove the configuration.

By default, no number template is bound to the local voice subscriber line in POTS view, no number template is configured for the terminating side when the POTS entity serves as a trunk, and no number template is configured for the voice entity in VoIP or VoFR entity view.

The number template defined by the **match-template** command can be used to match the number reaching the corresponding voice entity. The voice entity will complete the call if the match is successful. The number template can be defined flexibly. It can not only be a string of a unique number like 01016781234, but also an expression that can match a group of numbers, such as "010[1-5]678...". They

are used to match the actual numbers in the received call packets to complete the calls.

When configuring a POTS entity, use the **match-template** command to define the number template to be bound to the local voice entity. When configuring a VoIP entity, use the **match-template** command to define the number template on the called side.

In E1 voice, "T", "#", and "" are not supported currently.*

Example # Specify 5557922 as a telephone number of voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] match-template 5557922
```

Configure a match template for VoIP entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 010 voip
[Sysname-voice-dial-entity10] match-template 5557922
```

nlp-on

Syntax **nlp-on**

undo nlp-on

View Voice subscriber line view

Parameter None

Description Use the **nlp-on** command to enable the EC nonlinear processing function on a voice interface.

Use the **undo nlp-on** command to disable the function.

By default, the EC nonlinear processing function is enabled.

- *This command takes effect only after the **echo-canceller enable** command is configured.*
- *Currently, only digital voice subscriber lines support the **undo nlp-on** command, but analog voice subscriber lines do not.*

Example # Disable the EC nonlinear processing function on voice interface.

```
<Sysname> system-view
[Sysname] voice-setup
```

```
[Sysname-voice] subscriber-line 1/0
[Sysname-subscriber-line 1/0] undo nlp-on
```

outband

Syntax **outband** { **h225** | **h245** | **nte** }

undo outband

View POTS/VoIP entity view

Parameter **h225**: Adopts H.225 out-of-band to transmit DTMF.

h245: Adopts H.245 out-of-band to transmit DTMF.

nte: Adopts named telephone event (NTE) to transmit DTMF.

Description Use the **outband** command to configure out-of-band DTMF transmission.

Use the **undo outband** command to restore the default.

By default, the inband DTMF transmission mode is adopted.

Related command: **fast-connect** and **tunnel-on**.

Example # Configure DTMF out-of-band transmission in the fast connection mode for VoIP voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] fast-connect
[Sysname-voice-dial-entity10] outband h225
```

payload-size

Syntax **payload-size** { **g711** | **g723** | **g726r16** | **g726r24** | **g726r32** | **g726r40** | **g729** } *time-length*

undo payload-size { **g711** | **g723** | **g726r16** | **g726r24** | **g726r32** | **g726r40** | **g729** }

View POTS/VoIP/VoFR entity view

Parameter **g711**: Packetization period in milliseconds for **g711alaw** or **g711ulaw** codec, an integral multiple of 10 in the range of 10 to 30, with a default of 20.

g723: Packetization period in milliseconds for **g723r53** or **g723r63** codec, an integral multiple of 30 in the range of 30 to 180, with a default of 30.

g726r16: Packetization period in milliseconds for g726r16 codec, an integral multiple of 10 in the range of 10 to 110, with a default of 30.

g726r24: Packetization period in milliseconds for g726r24 codec, an integral multiple of 10 in the range of 10 to 70, with a default of 30.

g726r32: Packetization period in milliseconds for g726r32 codec, an integral multiple of 10 in the range of 10 to 50, with a default of 30.

g726r40: Packetization period in milliseconds for g726r40 codec, an integral multiple of 10 in the range of 10 to 40, with a default of 30.

g729: Packetization period in milliseconds for **g729r8** or **g729a** codec, an integral multiple of 10 in the range of 20 to 180, with a default of 30.

time-length: DSP packetization period for a codec.

Description Use the **payload-size** command to configure the voice packetization period for different codecs.

Use the **undo payload-size** command to restore the default.

By default, the voice packetization period for **g971** is 20 milliseconds, and that for **g723**, **g726**, and **g726** is 30 milliseconds.

In voice dial program view, you can configure global attributes for voice entities, namely, the default voice packetization period of the DSP for each codec.

Related command: **default entity payload-size**, **entity compression**.

Example # Set the voice packetization period of the DSP for g711 codec to 30 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] payload-size g711 30
```

Restore the default voice packetization period of the voice entity for g9711 codec.

```
[Sysname-voice-dial-entity10] undo payload-size g711
```

plc-mode

Syntax **plc-mode** { **general** | **specific** }

undo plc-mode

View Analog FXS/FXO voice subscriber line view

Parameter **general**: Uses the universal frame erasure algorithm.

specific: Uses the specific algorithm provided by the voice gateway.

Description Use the **plc-mode** command to configure a packet loss compensation mode for the analog FXS/FXO voice subscriber line.

Use the **undo plc-mode** command to restore the default.

By default, the gateway-specific algorithm is used for packet loss compensation.

Example # Configure the voice gateway to use the universal packet loss compensation algorithm.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] plc-mode general
```

receive gain

Syntax **receive gain** *value*

undo receive gain

View FXS/FXO/E&M voice subscriber line view

Parameter *value*: Voice input gain in dB, in the range of -14.0 to +13.9 with one digit after the decimal point.

Description Use the **receive gain** command to configure the gain value at the voice subscriber line input end.

Use the **undo receive gain** command to restore the default.

By default, the input gain on the voice interface is 0 dB.

This command is applicable to FXO, FXS, analog E&M subscriber lines and digital E1 voice subscriber line.

When the voice signal on the line attenuates to a relatively great extent, this command can be used to appropriately enhance the voice input gain.

Related command: **transmit gain** and **subscriber-line**.

Example # Configure the voice input gain as 3.5dB on subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] receive gain 3.5
```

CAUTION: *Gain adjustment may lead to a call failure. You are not recommended to adjust the gain. If necessary, do it with the guidance of technical personnel.*

register-number

Syntax **register-number**

undo register-number

View POTS entity view

Parameter None

Description Use the **register-number** command to enable the VoIP gateway to register numbers of a voice entity with an H.323 gatekeeper or SIP server.

Use the **undo register-number** command to disable a gateway from registering numbers of a voice entity with an H.323 gatekeeper or SIP server.

By default, the VoIP gateway registers numbers of the POTS voice entity with an H.323 gatekeeper (GK) or SIP server.

In some cases, you need to configure the same POTS entity on multiple gateways. As a GK and a SIP server cannot have the same number, you cannot register a POTS entity with a GK and a SIP server at the same time.

In other cases, you may need to register only some port numbers on the gateway with a GK or a SIP server to meet some special requirements. You can use the **undo register-number** command to specify the voice entity whose number does not need to be registered.

Related command: **match-template**.

Example # Specify the gateway not to register the numbers of POTS entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] undo register-number
```

reset voice cmc statistic

Syntax **reset voice cmc statistic**

View User view

Parameter None

Description Use the **reset voice cmc statistic** command to clear calling statistics on CMC module.

Related command: **display voice iva statistic**.

Example # Clear calling statistics on CMC module.

```
<Sysname> reset voice cmc statistic
```

reset voice ipp statistic

Syntax **reset voice ipp statistic**

View User view

Parameter None

Description Use the **reset voice ipp statistic** command to reset IPP statistics.

Related command: **display voice ipp statistic**.

Example # Clear IPP statistics.

```
<Sysname> reset voice ipp statistic
```

reset voice iva statistic

Syntax **reset voice iva**

View User view

Parameter None

Description Use the **reset voice iva statistic** command to clear IVA statistics.

Related command: **display voice iva statistic**.

Example # Clear IVA statistics.

```
<Sysname> reset voice iva statistic
```

rtp payload-type nte

Syntax **rtp payload-type nte** *value*

undo rtp payload-type nte

View POTS/VoIP entity view

Parameter *value*: Value of the payload type field in RTP packets, in the range of 96 to 127.

Description Use the **rtp payload-type nte** command to configure the payload type field in RTP packets in the case of DTMF relay using NTE.

Use the **undo rtp payload-type nte** command to restore the default.

By default, the payload type field in RTP packets is set to 101 in the case of DTMF relay using NTE.

- *It is forbidden to set the NTE payload type field to "98", which has already been used to identify nonstandard T38 fax packets.*
- *When the device is connected with devices of other manufacturers for communication, you cannot set the payload type field to any forbidden by these routers. Otherwise, an NTE negotiation failure may occur.*

Example # Set the NTE payload type field to "102" for VoIP entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] rtp payload-type nte 102
```

send-busytone

Syntax **send-busytone** { **enable** | **time** *seconds* }

undo send-busytone { **enable** | **time** }

View Analog FXO voice subscriber line view

Parameter **enable**: Enables busy-tone sending on the FXO interface.

time *seconds*: Duration of busy tone in seconds, in the range of 2 to 15. It defaults to 3 seconds. This parameter is not available without using the **send-busytone enable** command to enable busy-tone sending function.

Description Use the **send-busytone** command to enable busy tone sending on the FXO interface. Use the **undo send-busytone** command to disable busy tone sending on the FXO interface.

By default, busy tone sending is disabled.

Example # Enable FXO interface 1/0 to send busy tone that lasts 5 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] send-busytone enable
[Sysname-voice-line1/0] send-busytone time 5
```

send-ring

Syntax **send-ring**

undo send-ring

View Voice entity view

Parameter None

Description Use the **send-ring** command to enable the local end to play ringback tone.

Use the **undo send-ring** command to disable the local end to play ringback tone.

By default, the local end does not play ringback tone.

In VoIP view, this command is applicable only after the fast connection function is enabled. In POTS view, you can configure this command after you carry out the **line** command to bind a voice entity to a trunk (other than FXS voice subscriber line).

Example # Enable the local end to play ringback tone.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] fast-connect
[Sysname-voice-dial-entity10] send-ring
```

shutdown (voice entity view)

Syntax **shutdown**

undo shutdown

View POTS/VoIP entity view

Parameter None

Description Use the **shutdown** command to change the management status of the specified voice entity from UP to DOWN.

Use the **undo shutdown** command to restore the default management status of the voice entity.

By default, the voice entity management status is UP.

Running command **shutdown** will cause the voice entity unable to make calls.

Example # Change the status of voice entity 4 to DOWN.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 4 pots
[Sysname-voice-dial-entity4] shutdown
```

shutdown (voice subscriber line view)

Syntax **shutdown**

undo shutdown

View FXS/FXO/E&M voice subscriber line view

Parameter None

Description Use the **shutdown** command to set the voice subscriber line DOWN.

Use the **undo shutdown** command to restore the default status of the voice subscriber line.

By default, the voice subscriber line is UP.

This command is applicable to FXO, FXS, analog E&M subscriber lines and E1/T1 voice subscriber line.

The POTS interface on the voice interface card will be down and there will be no sound on the connected telephone after the command **shutdown** is executed, and whereas the specified voice subscriber line will be up after the **undo shutdown** command is executed.

Example # Shut down voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] shutdown
```

silence-th-span

Syntax **silence-th-span** *threshold time-length*

undo silence-th-span

View FXO subscriber line view

Parameter *threshold*: Silence threshold. If the amplitude of voice signal from the switch is smaller than this value, the system regards the voice signal as silence. This

threshold ranges from 0 to 200. Normally, the signal amplitude on the links without traffic is in the range of 2 to 5.

time-length: Silence duration for automatic on-hook. Upon expiration of this duration, the system goes on-hook automatically. It ranges from 2 to 7,200 seconds.

Description Use the **silence-th-span** command to set the silence duration for automatic on-hook.

Use the **undo silence-th-span** command to restore the default.

By default, the silence threshold is 3 and the silence duration for automatic on-hook is 7,200 seconds (namely, 2 hours).

Example # Set the silence threshold to 20 and the silence duration to 10 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] silence-th-span 20 10
```

slic-gain

Syntax **slic-gain** { **0** | **1** }

undo slic-gain

View Analog E&M voice subscriber line view

Parameter **0**: Sets the output gain of the subscriber line interface circuit (SLIC) chip to 0.8 dB.

1: Sets the output gain of the SLIC chip to 2.1 dB.

Description Use the **slic-gain** command to configure the output gain of the SLIC chip. The bottom layer tunes signal gain through the SLIC chip.

Use the **undo slic-gain** command to restore the default output gain.

By default, the output gain of the SLIC chip is 0 dB.

Example # Set SLIC-gain to 1 in analog E&M voice subscriber line view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] slic-gain 1
```

subscriber-line

Syntax **subscriber-line** *line-number*

View Voice view

Parameter *line-number:* Voice subscriber line number.

Description Use the **subscriber-line** command to enter analog FXS, FXO, and E&M, or digital E1/T1 voice subscriber line view.

Use the **subscriber-line** *line-number* command to enter the voice subscriber line view. For example, if *line-number* is an FXS voice subscriber line, the system will enter the FXS voice subscriber line view; if *line-number* is an analog E&M voice subscriber line, the system will enter analog E&M voice subscriber line view.

Example # Enter the view of the voice subscriber line 1/0 in voice view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0]
```

timer dial-interval

Syntax **timer dial-interval** *seconds*

undo timer dial-interval

View FXS/FXO/E&M voice subscriber line view

Parameter *seconds*: Maximum interval in seconds for dialing the next digit, in the range of 1 to 300.

Description Use the **timer dial-interval** command to configure the maximum interval for dialing the next digit.

Use the **undo timer dial-interval** command to restore the default setting.

By default, the maximum interval for dialing the next digit is 10 seconds.

This timer will restart each time the subscriber dials a digit and will work in this way until all the digits of the number are dialed. If the timer expires before the dialing is completed, the subscriber will be prompted to hook up and the call is terminated.

Example # Set the maximum duration waiting for the next digit on voice line 1/0 to 5 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] timer dial-interval 5
```

timer first-dial

Syntax **timer first-dial** *seconds*

undo timer first-dial

View FXS/FXO voice subscriber line view

Parameter *seconds*: Maximum interval in seconds between off-hook and dialing the first digit, in the range of 1 to 300.

Description Use the **timer first-dial** command to configure the maximum interval between off-hook and dialing the first digit.

Use the **undo timer first-dial** command to restore the default setting.

By default, the maximum interval between off-hook and dialing the first digit is 15 seconds.

Upon the expiration of the timer, the subscriber will be prompted to hook up and the call is terminated.

Example # Set the maximum interval between off-hook and dialing the first digit to 10 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] timer first-dial 15
```

timer hookoff-interval

Syntax **timer hookoff-interval** *milliseconds*

undo timer hookoff-interval

View FXO voice subscriber line view

Parameter *milliseconds*: Interval between on-hook and off-hook in milliseconds, in the range of 500 to 4,000.

Description Use the **timer hookoff-interval** command to configure the interval between on-hook and off-hook.

Use the **undo timer hookoff-interval** command to restore the default.

By default, the interval between on-hook and off-hook is 500 milliseconds.

In the delay off-hook mode, the on-hook/off-hook state between FXS and FXO voice subscriber lines is consistent. When an FXS voice subscriber line goes

off-hook, the bound FXO voice subscriber line goes off-hook, too. When the FXS voice subscriber line in the off-hook state needs to connect the FXO voice subscriber line to originate a call over PSTN, the FXO voice subscriber line must first perform an on-hook operation, and then perform an off-hook operation to send the called number.

Related command: **hookoff-mode**.

Example # Set the interval from on-hook to off-hook for FXO voice subscriber line 1/0 to 600 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] timer hookoff-interval 600
```

timer ring-back

Syntax **timer ring-back** *seconds*

undo timer ring-back

View FXS/FXO/E&M voice subscriber line view

Parameter *seconds*: Maximum duration in seconds of playing ringback tone, in the range of 5 to 120.

Description Use the **timer ring-back** command to configure the maximum duration of playing the ringback tone.

Use the **undo timer ring-back** command to restore the default.

By default, the maximum duration of playing the ringback tone is 60 seconds.

This command applies only on interfaces that are analog E&M, digital E&M, FXS, or FXO.

Example # Set the maximum time duration of playing ringback tones to eight seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] timer ring-back 8
```

timer wait-digit

Syntax **timer wait-digit** { *seconds* | **infinity** }

undo timer wait-digit

View E&M voice subscriber line view

Parameter *seconds*: Maximum duration in seconds the system waits for a digit, in the range of 3 to 600.

infinity: Infinite time.

Description Use the **timer wait-digit** command to configure the maximum time duration the system waits for a digit.

Use the **undo timer wait-digit** command to restore the default time settings.

By default, the maximum time duration the system waits for a digit is 5 seconds.

Example # Set the maximum duration waiting for the first dial on voice line 1/0 to 5 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] timer wait-digit 5
```

transmit gain

Syntax **transmit gain** *value*

undo transmit gain

View FXS/FXO/E&M voice subscriber line view

Parameter *value*: Voice output gain in dB, in the range of -14.0 to 13.9 with one digit after the decimal point.

Description Use the **transmit gain** command to configure the voice subscriber line output end gain value.

Use the **undo transmit gain** command to restore the default value.

By default, the output gain on the voice interface is 0 dB.

When a relatively small voice signal power is needed on the output line, this command can be used to properly increase the voice output gain value to adapt to the output line signal requirement.

Related command: **receive gain** and **subscriber-line**.

CAUTION: Gain adjustment may lead to a call failure. You are not recommended to adjust the gain. If necessary, do it with the guidance of technical personnel.

Example # Configure the voice output gain value as -6.7dB on subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] transmit gain -6.7
```

tunnel-on

Syntax **tunnel-on**

undo tunnel-on

View VoIP entity view

Parameter None

Description Use the **tunnel-on** command to enable tunnel function.

Use the **undo tunnel-on** command to disable tunnel function.

By default, the tunnel function is disabled.

Tunnel function can assist in negotiating process of such nonstandard H.245 message as transmitting DTMF digit transparently.

Only after successfully enabling H.323 fast connection mode, can you fulfill the configuration of tunnel function. Being the calling gateway, it can be decided whether or not to enable the tunnel function for each call on the router. Being the called gateway, it shall be decided whether or not to enable the tunnel function based on the status of the calling gateway. That is, if the function is enabled on calling gateway, it will also be enabled on the called gateway. Otherwise, tunnel function is disabled on both sides. To implement this function, you need to carry out the **voip called-tunnel enable** command to enable the fast connection function on the terminating gateway.

During actual configuration, it is only necessary to fulfill this command for the VoIP voice entity at the calling gateway.

Related command: **fast-connect**, **outband**, **voip called-tunnel enable** and **voip called-start**.

Example # Enable the tunnel function for VoIP voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] fast-connect
[Sysname-voice-dial-entity10] tunnel-on
```

type

Syntax **type** { **1** | **2** | **3** | **5** }

undo type

View Analog E&M voice subscriber line view

Parameter **1, 2, 3** and **5**: Correspond respectively to the four signal types of analog E&M subscriber lines, i.e. type 1, 2, 3 and 5.

Description Use the **type** command to configure the analog E&M subscriber line signal type.

Use the **undo type** command to cancel the existing settings.

By default, the analog E&M subscriber line signal type is type 5.

This command is only applicable to the analog E&M subscriber line.

Example # Configure subscriber line 1/0 analog E&M subscriber line type as type 3.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0
[Sysname-voice-line1/0] type 3
```

vad-on

Syntax **vad-on**

undo vad-on

View POTS/VoIP/VoFR entity view

Parameter None

Description Use the **vad-on** command to enable voice activity detection (VAD) function.

Use the **undo vad-on** command to disable silence detection function.

By default, the silence detection function is disabled.

Note that G.711 codec does not support VAD.

The voice activity detection (VAD) discriminates between silence and speech on a voice connection according to their energies. VAD reduces the bandwidth requirements of a voice connection by not generating traffic during periods of silence in an active voice connection. Speech signals are generated and transmitted only when an active voice segment is detected. Researches show that VAD can save the transmission bandwidth by 50%.

Related command: **cng-on**.

Example # Enable VAD on POTS voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] vad-on
```

vi-card busy-tone-detect

Syntax **vi-card busy-tone-detect** { **auto** *index line-number* | **custom** *area-number index argu f1 f2 p1 p2 p3 p4 p5 p6 p7* }

undo vi-card busy-tone-detect custom *index*

View Voice view

Parameter *index*: Index of busy tone type, in the range of 0 to 3.

line-number: Voice subscriber line number. The value range varies with the inserted cards.

area-number: Area number. Currently, it is set to **2**.

argu: Reserved, in the range of 0 to 32,767.

f1: Frequency 1 in Hz, in the range of 50 to 3,600.

f2: Frequency 2 in Hz, in the range of 50 to 3,600.

p1: Signal amplitude 1, in the range of 50 to 32,767.

p2: Signal amplitude 2, in the range of 50 to 32,767.

p3: Duration of a single tone in milliseconds, in the range of 10 to 1,000.

p4: Duration error of a single tone in milliseconds, in the range of 0 to 500.

p5: Duration of silence in milliseconds, in the range of 10 to 1,000.

p6: Duration error of silence in milliseconds, in the range of 0 to 500.

p7: Absolute difference between *p3* and *p5* in milliseconds, in the range of 0 to 500

Description Use the **vi-card busy-tone-detect** command to configure the parameters for the busy tone detection on the FXO interface.

Use the **undo vi-card busy-tone-detect** command to restore the default settings.

This command applies to the FXO interface only.

The system supports four types of busy tones, which are specified by the *index* argument.

When detecting a busy tone on the FXO interface, the system will automatically calculate the parameters related to busy tone detection. You can use the **display current-configuration** command to displays the settings of these parameters.

CAUTION: *After you use the* ***vi-card busy-tone-detect custom*** *command to configure the parameters related to the busy tone detection, these parameters do not take effect immediately. The manually configured busy tone parameters can take effect only after you execute the* ***area custom*** *command in voice view.*

Related commands: **area custom**.

Examples # Enable the automatic busy tone detection on subscriber line 2, with the busy tone index being 0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vi-card busy-tone-detect auto 0 2/0
```

Save the frequency of the busy tone indexed as 0, duration limit of high/low level, duration error of high/low level, and duration difference of high/low level.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vi-card busy-tone-detect custom 2 0 99 450 450 8000
8000 800 300 500 500 500
```

vi-card cptone-custom

Syntax **vi-card cptone-custom** { **busy-tone | congestion-tone | dial-tone | ringback-tone | special-dial-tone | waiting-tone** } *comb freq1 freq2 time1 time2 time3 time4*

undo vi-card cptone-custom { **all | busy-tone | congestion-tone | dial-tone | ringback-tone | special-dial-tone | waiting-tone** }

View Voice view

Parameter **busy-tone**: Busy tone.

congestion-tone: Congestion tone.

dial-tone: Dial tone.

ringback-tone: Ringback tone.

special-dial-tone: Special dial tone.

waiting-tone: Call waiting tone.

comb: Combination mode, in the range of 0 to 2. The values 0, 1, and 2 represent the superimposition and modulation of two frequencies, and alternation between two frequencies, respectively.

freq1 and *freq2*: Two frequencies in Hz. The frequency range is related to the combination mode. In the case of frequency superimposition or alternation, the two frequencies fall in the range of 300 Hz to 3,400 Hz. In the case of frequency modulation, the two frequencies fall in the range of 300 Hz to 3,400 Hz, and the sum of and the absolute difference between the two frequencies also fall in this range.

time1: Make time for the first make-to-break ratio in milliseconds, in the range of 30 to 8,192. In the case of continuous play, the value is 8,192.

time2: Break time for the first make-to-break ratio in milliseconds, 0 or 30 through 8,191.

time3: Make time for the second make-to-break ratio in milliseconds, 0 or 30 through 8,191.

time4: Break time for the second make-to-break ratio in milliseconds, 0 or 30 to 8,191.

index: Index of busy tone type, in the range of 0 to 3.

Description Use the **vi-card cptone-custom** command to configure parameters for a customized call progress tone.

Use the **undo vi-card cptone-custom** command to remove the configuration.

By default, no customized call progress tone is configured.

After you configure parameters for a customized call progress tone, they do not take effect immediately. They do only after you execute the **cptone country-type CS** command in voice view.

Example # Customize parameters for a busy tone, with the two frequencies both being 425 Hz, and the make time and break time both being 350 milliseconds.

```
<sysname> system-view
[sysname] voice-setup
[sysname-voice] vi-card cptone-custom busy-tone 0 425 425 350 350 350 350
```

vi-card reboot

Syntax **vi-card reboot** *slot-number*

View Voice view

Parameter *slot-number*: Number of the slot where the voice card is located.

Description Use the **vi-card reboot** command to reboot a voice card.

First use command **display version** or **display device** to display the distributed slots of the voice cards in the router.

Related command: **display version** on page 2417, and **display device** on page 2251.

CAUTION: You can use this command to reset only the analog voice cards of SIC and MIM. To reset digital voice card and FIC analog voice card, carry out the reboot slot slot-number command in system view.

Example # Reset the voice card of slot 3.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vi-card reboot 3
```

voice-setup

Syntax **voice-setup**

View System view

Parameter None

Description Use the **voice-setup** command to enter voice view and enable voice services.

Example # Enter voice view and enable voice services.

```
<Sysname> system-view
[Sysname] voice-setup
```

voip called-tunnel enable

Syntax **voip called-tunnel enable**

undo voip called-tunnel enable

View Voice view

Parameter None

Description Use the **voip calledtunnel enable** command to enable the tunnel function on the called gateway.

Use the **undo voip calledtunnel enable** command to disable the tunnel function on the called gateway.

By default, the tunnel function on the called gateway is enabled.

Related command: **tunnel-on**.

*If the **voip called-start** normal command is configured, the **voip called-tunnel enable** command is unavailable.*

Example # Disable the tunnel function on the called gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] undo voip called-tunnel enable
```

voip called-start

Syntax **voip called-start** { **fast** | **normal** }

undo voip called-start

View Voice view

Parameter **fast**: The called GW initializes calls in a fast way.

normal: The called GW initializes calls in a non-fast way.

Description Use the **voip call-start** command to configure a call initialization mode for the called GW.

Use the **undo voip call-start** command to restore the default.

By default, the fast connection mode is used for call initialization.

As the process of faculty negotiation is omitted in fast connection procedures, the faculties of the two parties are determined by the GW. If a router acts as a calling GW, you can enable or disable fast connection for each channel of initiated calls. If it acts as a called GW, it will use or not use the fast connection mode to initialize calls depending on the parameters of the **voip call-start** command, in the case that the calling GW uses the fast connection mode.

Related command: **fast-connect**.

Example # Configure the called gateway to initialize calls in normal mode.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] voip called-start normal
```

voip timer

Syntax **voip timer voip-to-pots** *time*

undo voip timer voip-to-pots

View Voice view

Parameter **voip-to-pots** *time*: Duration in seconds for switching from a VoIP entity to a backup POTS entity after a call failure, in the range of 3 to 30.

Description Use the **voip timer** command to set the duration for switching from a VoIP entity to a backup POTS entity after a VoIP call failure.

Use the **undo voip timer** command to restore the default.

By default, the duration for switching from a VoIP entity to a backup POTS entity after a call failure is 5 seconds.

Example # Configure the duration for switching from a VoIP entity to a backup POTS entity after a call failure to 3 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] voip timer voip-to-pots 3
```

vqa dscp

Syntax **vqa dscp** { **media** | **signal** } *dscp-value*

undo vqa dscp { **media** | **signal** }

View Voice view

Parameter **media**: Global DSCP value in the ToS field of the IP packets that carry RTP streams.

signal: Global DSCP value in the ToS field of the IP packets that carry voice signaling.

dscp-value: DSCP value in the range 0 to 63 or the keyword **af11**, **af12**, **af13**, **af21**, **af22**, **af23**, **af31**, **af32**, **af33**, **af41**, **af42**, **af43**, **cs1**, **cs2**, **cs3**, **cs4**, **cs5**, **cs6**, **cs7**, or **ef**.

Table 684 DSCP values

Keyword	DSCP value in binary	DSCP value in decimal
af11	001010	10
af12	001100	12
af13	001110	14
af21	010010	18
af22	010100	20
af23	010110	22
af31	011010	26
af32	011100	28
af33	011110	30
af41	100010	34
af42	100100	36
af43	100110	38
cs1	001000	8
cs2	010000	16

Table 684 DSCP values

Keyword	DSCP value in binary	DSCP value in decimal
cs3	011000	24
cs4	100000	32
cs5	101000	40
cs6	110000	48
cs7	111000	56
default	101110	46
ef	101110	46

Description Use the **vqa dscp** command to globally set the DSCP subfield in the ToS field in IP packets that carry the RTP stream or voice signaling.

Use the **undo dscp media** command to restore the default.

By default, the DSCP subfield is set to **ef**, namely, 101110.

The function of this command is the same as the command used for setting DSCP in the "QoS" part of this manual. If two DSCP values are configured, the one configured in the "QoS" part takes priority.

Example # Set the DSCP value in the ToS field in the IP packets that carry voice signaling to af41.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vqa dscp signal af41
```

vqa dsp-monitor buffer-time

Syntax **vqa dsp-monitor buffer-time** *time*

undo vqa dsp-monitor buffer-time

View Voice view

Parameter **buffer-time** *time*: Duration in milliseconds of monitoring DSP buffer data, in the range 180 to 480.

Description Use the **vqa dsp-monitor buffer-time** command to set duration of monitoring DSP buffered data.

Use the **undo vqa dsp-monitor buffer-time** command to remove the setting.

By default, DSP buffered data is not monitored.

Duration greater than 240 milliseconds is recommended because too small a duration value will result in poor voice quality in the case of severe jitter.

Example # Set the duration of monitoring DSP buffered data to 270 milliseconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vqa dsp-monitor buffer-time 270
```

174 DIAL PLAN CONFIGURATION COMMANDS

caller-permit

Syntax **caller-permit** *calling-string*

undo caller-permit { *calling-string* | **all** }

View POTS/VoIP/VoFR entity view

Parameter **all**: Specifies all calling numbers.

calling-string: Calling number permitted to originate a call to the local voice entity, in the format of { [**+**] string [**$**] }| **$**, with a maximum length of 32 characters. The following describes the symbols in the format:

- +: Plus sign. It comes before the whole number and indicates that the number is an E.164 number.
- $: Dollar sign. When it comes at the end of a number, the calling number must completely match the part before the dollar sign. When it comes alone, the calling number can be null.
- If there is no sign behind the number, number segments beginning with it are permitted to originate calls.
- *string*: A character string consisting of 0123456789#*.!+%[]()-. Table 685 describes these characters.

Table 685 Description of characters in a string

Character	Meaning
0-9	Digits 0 through 9
# and *	Indicates a valid digit each
.	Wildcard, which can match any valid digit. For example, 555.... can match any number beginning with 555 and ending in four additional characters.
!	Indicates the sub-expression before it appears once or does not appear. For example, 56!1234 can match 51234 and 561234.
+	Indicates the sub-expression before it appears one or more times. If the plus sign (+) appears at the head of a number, the number is an E.164 number and the plus sign itself does not represent a specific number or number repetition. For example, 9876(54)+ can match 987654, 98765454, 9876545454, and so on, and +110022 is an E.164-compliant number.
-	Hyphen (connecting element), used to connect two numbers (The smaller comes before the larger) to indicate a range of numbers, for example, 1-9 inclusive.

Table 685 Description of characters in a string

Character	Meaning
%	Indicates the sub-expression before it appears multiple times or does not appear. For example, 9876(54)% can match 9876, 987654, 98765454, 9876545454, and so on.
[ ]	Indicates a range for matching. For example, [1-36A] indicates a single character among 1, 2, 3, 6, and A can be matched.
( )	Indicates a string of characters. For example, (123) indicates the character string 123. It is usually used together with signs such as !, %, or +. For example, 408(12)+ can match the character string 40812 or 408121212, but not 408 (that is, the string 12 can appear repeatedly and must appear once).

The sub-expression (one digit or digit string) before signs such as !, %, and + is used for imprecise match. The processing of these signs is similar to that of the wildcard ".". These signs must follow a valid digit or digit string and cannot exist independently.

If embedded, signs "[ ]" and "( )" must be presented in the form of "([ ])". The forms of "[[ ]]" and "[( )]" are incorrect.

The sign "-"can present itself only in "[ ]" and characters at the two ends must be of the same type.

Description Use the **caller-permit** command to configure a calling number permitted to originate calls to the local voice entity.

Use the **undo caller-permit** command to remove the configuration.

By default, no calling number is configured, that is, incoming calls are not restricted.

At most 32 calling numbers are permitted to originate calls to a voice entity.

Related command: **match-template** on page 2599.

Example # Configure voice entity 2 to accept calls from the number 660268.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 2 pots
[Sysname-voice-dial-entity2] caller-permit 660268$
```

Configure voice entity 2 to accept calls from the number beginning with "20".

```
[Sysname-voice-dial-entity2] caller-permit 20
```

dial-prefix

Syntax **dial-prefix** *string*

undo dial-prefix

View POTS entity view

Parameter *string*: Prefix code, a character string consisting of up to 31 characters that can include 0 through 9, #, and *. Table 686 describes these characters:

Table 686 Description of characters in the string argument

Character	Meaning
0-9	Digits 0 through 9.
,	One comma represents a pause of 500 milliseconds and it can be positioned anywhere in a number.
# and *	Indicates a valid digit each.

Description Use the **dial-prefix** command to configure a dial prefix for a voice entity.

Use the **undo dial-prefix** command to remove the configured prefix.

By default, no dial prefix is configured.

The configuration of the PBX connected to the originating router determines whether a two-stage dialing tone is played or not.

When a voice router receives a voice call, it will compare the numbers in the match-templates of its own POTS entities with the received called number and select one POTS entity to process the call. If a prefix is configured, the voice router will send the prefix and dialed number together through the FXO interface. For details about number sending, refer to "send-number" on page 2642.

When the number with a prefix exceeds 31 digits, only the first 31 digits are sent.

Related command: **match-template** on page 2599 and **send-number**.

Example # Specify 0 as a prefix.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 3 pots
[Sysname-voice-dial-entity3] dial-prefix 0
```

display voice number-substitute

Syntax **display voice number-substitute** [*list-tag*]

View Any view

Parameter *list-tag*: Serial number of a number substitution rule list, in the range of 1 to 2147483647.

Description Use the **display voice number-substitute** command to display the configuration information of a number substitution rule list.

Related command: **number-substitute**.

Example # Display the configuration information of all number substitution rule lists.

```
<Sysname> display voice number-substitute
  Current configuration of number-substitute
  #
    ************ NUMBER-SUBSTITUTE ************
      List-tag   : 4
      First-rule : INDEX_INVALID
      Dot-match  : left-right
      rule 1
        Input-format   : ^011408
        Output-format  : 1408
    #
  End
```

dot-match

Syntax **dot-match** { **end-only** | **left-right** | **right-left** }

undo dot-match

View Voice number-substitute view

Parameter **end-only**: Reserves the digits which all ending dots (.) in the number input format correspond to.

left-right: Reserves from left to right the digits which the dots in the number input format corresponds to.

right-left: Reserves from right to left the digits which the dots correspond to in a number.

Description Use the **dot-match** command to configure the dot match rule of the number substitution rule list.

Use the **undo dot-match** command to restore the dot match rule to the default.

This command only applies to the rules of the number substitution rule list in current view.

By default, the dot match rule is **end-only**.

The dots here are virtual match digits. Virtual match digits refer to those matching the variable part such as ., +, %, !, and [] in a regular expression. For example, when 1255 is matched with the regular expression 1[234]55, the virtual match digit is 2, when matched with the regular expression 125+, the virtual match digit is 5, and matched with the regular expression 1..5, the virtual match digits are 25.

For details about the dot match rule of the number substitution rule list, refer to "rule" on page 2634.

Example # Set the dot match rule of number substitution rule list 20 to **right-left**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-substitute 20
[Sysname-voice-dial-substitute20] dot-match right-left
```

first-rule

Syntax **first-rule** *rule-number*

undo first-rule

View Voice number-substitute view

Parameter *rule-number*: Serial number of a number substitution rule (namely, the serial number of a number substitution rule configured by using the **rule** command), in the range of 0 to 31.

Description Use the **first-rule** to configure a preferred number substitution rule in the current number substitution rule list.

Use the **undo first-rule** command to remove the configured preferred number substitution rule.

By default, no preferred number substitution rule is configured.

In a voice call, the system first uses the rule defined by the **first-rule** command for number substitution. If this rule fails to apply or is not configured, it will try to apply all other rules in order until one or none of them applies.

Example # Specify rule 4 in number substitution list 20 as the preferred rule.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-substitute 20
[Sysname-voice-dial-substitute20] rule 4 663 3
[Sysname-voice-dial-substitute20] first-rule 4
```

max-call (in voice dial program view)

Syntax **max-call** *set-number max-number*

undo max-call { *set-number* I **all** }

View Voice dial program view

Parameter *set-number*: Number identifying a maximum-call-connection set, in the range of 1 to 2,147,483,647. At most 256 maximum-call-connection sets can be configured.

max-number: Maximum number of call connections in a maximum-call-connection set, in the range of 1 to 120.

all: Specifies all the maximum-call-connection sets.

Description Use the **max-call** command to configure maximum-call-connection sets.

Use the **undo max-call** command to remove the specified maximum-call-connection set or all maximum-call sets.

By default, no maximum-call-connection sets are configured.

Together with the **max-call** command in voice entity view, this command is used to limit the maximum number of call connections of a voice entity or a set of voice entities.

Related command: **max-call (in voice entity view)**.

Example # Set the maximum number of call connections in maximum-call-connection set 1 to 5.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] max-call 1 5
```

max-call (in voice entity view)

Syntax **max-call** *set-number*

undo max-call

View POTS/VoIP/VoFR voice entity view

Parameter *set-number*: Number identifying a maximum-call-connection set (number of the maximum-call-connection set configured in voice dial program view), in the range of 1 to 2147483647.

Description Use the **max-call** command to bind a voice entity to the maximum-call-connection set specified by the *set-number* argument.

Use the **undo max-call** command to remove the binding. Although you can bind each voice entity to only one maximum-call-connection set, you can change the binding.

By default, no maximum-call-connection set is bound, that is, there is no limitation on the number of call connections.

This command is used together with the **max-call** command in voice dial program view. The former is used to bind a voice entity to a maximum-call-connection set,

while the latter is used to configure a serial number for a maximum-call-connection set and the maximum number of call connections.

Related command: **max-call (in voice dial program view)**.

Example # Bind voice entity 10 to maximum-call-connection set 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] max-call 1 5
[Sysname-voice-dial] max-call 1 5
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] max-call 1
```

number-match

Syntax **number-match** { **longest** | **shortest** }

undo number-match

View Voice dial program view

Parameter **longest**: Matches the longest number.

shortest: Matches the shortest number.

Description Use the **number-match** command to configure a global number match policy.

Use the **undo number-match** command to restore the default number match policy.

By default, the shortest-number match policy is adopted.

Related command: **match-template** on page 2599 and **terminator**.

*If the longest-number match policy is configured and the **rule** command with the input-format argument ending in a dollar sign ($) is carried out, after a user dials a number, the system will not look up the voice entity to connect the call until the dialing interval expires. Because the dollar sign ($) requires that the last digit configured should match the last one dialed, the system can determine the last dialed digit only after the dialing interval expires and the system stops collecting digits.*

Example # Configure the longest-number match policy.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-match longest
```

number-priority

Syntax **number-priority peer enable**

undo number-priority peer

View Voice dial program view

Parameters None

Description Use the **number-priority peer enable** command to match a number against a voice entity match template first.

Use the **undo number-priority peer** command to restore the default.

By default, a number starting with "*" or "#" will first match against a service feature code.

Examples # Configure a number to first match against a voice entity match template.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-priority peer enable
```

number-substitute

Syntax **number-substitute** *list-number*

undo number-substitute { *list-number* | **all** }

View Voice dial program view

Parameter *list-number*: Serial number of a number substitution rule list, in the range of 1 to 2147483647.

all: Specifies all number substitution rule lists.

Description Use the **number-substitute** command to create a number substitution rule list and enter voice number-substitute view.

Use the **undo number-substitute** command to remove a specified number substitution rule or all number substitution rule lists.

By default, no number substitution rule list is configured.

Related command: **rule** and **substitute (voice dial program view)**.

Example # Enter the voice dial program view and create a number substitution rule list.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-substitute 1
[Sysname-voice-dial-substitute1]
```

priority

Syntax **priority** *priority-order*

undo priority

View Voice entity view

Parameter *priority-order*: Priority of a voice entity, in the range of 0 to 10. The smaller the value, the higher the priority.

Description Use the **priority** command to configure the priority of a voice entity.

Use the **undo priority** command to restore the priority of a voice entity to the default.

By default, the priority level is 0.

If you have configured priority levels for voice entities and the selection priority rules (see "select-rule rule-order" on page 2638, "select-rule search-stop" on page 2639, and "select-rule type-first" on page 2640), the router will first select the voice entity with the highest priority to initiate a call. When this voice entity fails, the router will select a voice entity with the second highest priority to initiate a call.

Example # Set the priority level of voice entity 10 to 5.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] priority 5
```

private-line

Syntax **private-line** *string*

undo private-line

View FXS/FXO/E&M voice subscriber line view

Parameter *string*: E.164 telephone number of the terminating end, a string of 31 digits/characters, which can include 0 through 9, "*" and "#".

Description Use the **private-line** command to configure the private line auto ring-down (PLAR) function.

Use the **undo private-line** command to disable the private line auto ring-down function.

This function is disabled by default.

This command is applicable to FXO, FXS, analog E&M interface and digital E1 voice interface.

Example # Configure the private line auto ring-down function on voice subscriber line 1/0 so that 5559262 is automatically dialed out when the subscriber picks up the phone.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line1/0
[Sysname-voice-line1/0] private-line 5559262
```

rule

Syntax **rule** *rule-tag input-number output-number* [**number-type** *input-number-type output-number-type* | **numbering-plan** *input-numbering-plan output-numbering-plan*] *

undo rule { *rule-tag* | **all** }

View Voice number-substitute view

Parameter **all**: Deletes all number substitution rules.

rule-tag: Number identifying a substitution rule, in the range of 0 to 31.

input-number: Input string of a number involved in number substitution, in the format of [**^**] [+] *string* [$], up to 31 characters. The signs are explained as follows:

- Caret (^): The match begins with the first character of a number string. That is, the router begins with the first character of the match string to match a user number.
- Plus sign (+): It appears before a number, indicating that the number is an E.164 number.
- Dollar sign ($): It indicates that the last character of the match string must be matched. That is, the last digit of a user number must be matched with the last character of the match string.
- *string*: String consisting of characters such as 0 to 9, #, *, ., !, and %. Table 687 explains these characters:

Table 687 Meanings of characters in the string argument

Character	Meaning
0-9	Digit 0 through 9.
# and *	Valid digit each.
.	Wildcard, which can match any valid digit. For example, 555.... can match any number beginning with 555 and ending up with four additional characters.
!	The character or sub-expression before the sign does not appear or appears only once. For example, 56!1234 can match 51234 and 561234.
+	The character or sub-expression before the plus sign can appear one or more times. However, if the plus sign appears at the head of a number, the number is an E.164 number and the plus sign itself does not represent a specific number or number repetition. For example, 9876(54)+ can match 987654, 98765454, 9876545454, and so on, and +110022 is an E.164 number.
%	The character or sub-expression before the percent sign does not appear or appears multiple times. For example, 9876(54)% can match 9876, 987654, 98765454, 9876545454, and so on.

output-number: Output string of a number involved in number substitution, consisting of characters such as 0 to 9, #, *, and ., up to 31 characters. The characters are described in Table 687.

The sub-expression (one digit or digit string) before !, %, or + is not exactly-matched digit(s) and is handled in a similar way the wildcard (.). These signs cannot be used alone and must be preceded by a valid digit or digit string.

The dot (.) in the *input-number* and *output-number* arguments is handled in three ways:

1 The dot (.) in the *output-number* argument is considered invalid. If you use the **dot-match** command to set the dot match rule to **end-only** (that is, only dots at the end of the *input number* are handled), the dots in the *output-number* argument are discarded immediately, and the digits which all the dots at the end of the *input number* correspond to are added to the end of the *output number*.

2 Extra dots in the *output-number* argument are discarded. If you use the **dot-match** command to set the dot match rule to **right-left** (from right to left) or **left-right** (from left to right), and the number of dots in the *output-number* argument is greater than that in the *input-number* argument, all digits which the dots in the *input-number* argument correspond to are selected to replace the dots in the *output-number* argument one by one from right to left (or from left to right). The remaining dots (that are not replaced) in the *output-number* argument are discarded.

3 Extra dots in the *input-number* argument are discarded. If you use the **dot-match** command to set the dot match rule to **right-left** (from right to left) or **left-right** (from left to right), and the number of dots in the *input-number* argument is greater than or equal to that in the *output-number* argument, the dot handling includes two cases:

- For the right-left dot match rule, digits which the dots in the *input-number* argument correspond to are extracted from right to left according to the number of dots in the *output-number* argument to replace the dots in the *output-number* argument one by one. The digits that are not extracted in the *input-number* argument are discarded.

- For the left-right dot match rule, digits which the dots in the *output-number* argument correspond to are extracted from left to right according to the number of dots in the *output-number* argument to replace the dots in the *output-number* argument one by one. The digits that are not extracted in the *input-number* argument are discarded. Note that the right-left and left-right dot match rules are only applicable to the dot handling in the *input number* argument and that the extracted digits will always replace the dots in the *output-number* argument from left to right.

number-type: Specifies the type of a number.

input-number-type: Type of an input number involved in number substitution. For the values, see Table 688.

Table 688 Input number type

Number type	Description
abbreviated	Abbreviated number
any	Any number
international	International number
national	National number, but not a local network
network	Specific service network number
reserved	Reserved number
subscriber	Local network number
unknown	Number of an unknown type

output-number-type: Type of an output number involved in number substitution. For the values, see Table 689.

Table 689 Output number type

Number type	Description
abbreviated	Abbreviated number
international	International number
national	National number, but not a local network number
network	Specific service network number
reserved	Reserved number
subscriber	Local network number
unknown	Number of an unknown type

numbering-plan: Specifies a numbering plan.

input-numbering-plan: Input numbering plan involved number substitution. For the values, see Table 690.

Table 690 Input numbering plan

Numbering plan	Description
any	Any numbering plan
data	Data numbering plan

Table 690 Input numbering plan

Numbering plan	Description
isdn	ISDN telephone numbering plan
national	National numbering plan
private	Private numbering plan
reserved	Reserved numbering plan
telex	Telex numbering plan
unknown	Unknown numbering plan

output-numbering-plan: Numbering plan for an output number involved in number substitution. For the values, see Table 691.

Table 691 Output numbering plan

Numbering plan	Description
data	Data numbering plan
isdn	ISDN telephone numbering plan
national	National numbering plan
private	Private numbering plan
reserved	Reserved numbering plan
telex	Telex numbering plan
unknown	Unknown numbering plan

Description

Use the **rule** command to configure a number substitution rule.

Use the **undo rule** command to remove a specified number substitution rule or all number substitution rules.

By default, no number substitution rule is configured.

After you create a number substitution rule list successfully, you need to use this command to configure specific number-substitute rules for it.

Related command:

substitute (voice dial program view), **number-substitute**, **first-rule**, and **dot-match**.

Example

Configure number substitution rules for number substitution rule list 1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] number-substitute 1
```

Configure number substitution rule 1 for number substitution rule list 1 as follows:

- Input number: 91
- Output number: 1

```
[Sysname-voice-dial-substitute1] rule 1 ^91 1
```

Configure number substitution rule 2 for number substitution rule list 1 as follows:

- Input number: 92
- Output number: 2

```
[Sysname-voice-dial-substitute1] rule 2 ^92 2
```

Configure number substitution rule 3 for number substitution rule list 1 as follows:

- Input number: 93
- Output number: 3

```
[Sysname-voice-dial-substitute1] rule 3 ^93 3
```

Configure number substitution rule 3 for number substitution rule list 1 as follows:

- Input number: 93
- Output number: 3
- Input number type: any
- Output number type: International
- Input numbering plan: any
- Output numbering plan: telex.

```
[Sysname-voice-dial-substitute1] rule 3 ^93 3 number-type any intern
ational numbering-plan any telex
```

select-rule rule-order

Syntax **select-rule rule-order** *1st-rule* [*2nd-rule*] [*3rd-rule*]

undo select-rule rule-order

View Voice dial program view

Parameter *1st-rule*: First rule in the match order for voice entity selection. The value ranges from 1 to 4.

2nd-rule: Second rule in the match order for voice entity selection. The value ranges from 1 to 4 but differs from that of *1st-rule*.

3rd-rule: Third rule in the match order for voice entity selection. The value ranges from 1 to 4 but differs from those of *1st-rule* and *2nd-rule*.

Table 692 describes the meanings of integers 1 through 4.

Table 692 Meanings of integers

Integer	Meaning	Description
1	Exact match	The more digits of a digit string are matched from left to right, the higher the precision is. The system stops using the rule once a digit cannot be matched uniquely.
2	Priority	Voice entity priorities are divided into 11 levels numbered from 0 to 10. The smaller the value is, the higher the priority is. That means level 0 has the highest priority.
3	Random selection	The system selects at random a voice entity from a set of qualified voice entities.
4	Longest idle time	The longer the voice entity is idle, the higher the priority is.

Description Use the **select-rule rule-order** command to configure rules in the match order for voice entity selection.

Use the **undo select-rule rule-order** command to restore a rule in the match order for voice entity selection to the default.

By default, the match order for voice entity selection priority is exact match->voice entity priority -> random selection.

You can use the **select-rule rule-order** command to configure at most three different rules. The match order determines the sequence of rules:

- If there are multiple rules, the system first selects a voice entity according to the first rule.
- If the first rule cannot distinguish the priorities of voice entities, the system applies the second rule. If the second rule cannot still distinguish the priorities of voice entities, the system applies the third rule.
- If all the rules cannot distinguish the voice entity priorities, the system selects a voice entity with the smallest ID.

After the random selection rule is applied, there will be no voice entity selection conflict. Therefore, the random selection rule can only serve as a rule with the lowest priority or serve as a unique rule separately.

Related command: **select-rule search-stop**, **select-rule type-first**, and **priority**.

Example # Set the rules in the sequence of exact match->priority->longest idle time.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] select-rule rule-order 1 2 4
```

select-rule search-stop

Syntax **select-rule search-stop** *max-number*

undo select-rule search-stop

View Voice dial program view

Parameter *max-number*: Maximum number of voice entities found, in the range 1 to 128.

Description Use the **select-rule search-stop** command to configure the maximum number of voice entities found.

Use the **undo select-rule search-stop** command to restore the maximum number of voice entities found to 128.

By default, the maximum number of voice entities found is 128.

The **select-rule search-stop** command is used to define the maximum number of qualified voice entities to be found before the search stops. Even if the number of voice entities meeting call requirements is greater than max-number, the system will make call attempts to only the maximum number (max-number) of voice entities that are matched in accordance with rules.

Related command: **select-rule rule-order** and **select-rule type-first**.

Example # Configure the maximum number of voice entities found to 5.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] select-rule search-stop 5
```

select-rule type-first

Syntax **select-rule type-first** *1st-type 2nd-type 3rd-type*

undo select-rule type-first

View Voice dial program view

Parameter *1st-type*: Serial number of the type of the first priority, in the range of 1 to 3. Table 693 describes these values:

2nd-type: Serial number of the type of the second priority, in the range of 1 to 3. The value must be different from that of *1st-type*.

3rd-type: Serial number of the type of the third priority, in the range of 1 to 3. The value must be different from that of *1st-type* and *2nd-type*.

Table 693 describes the meanings of these values.

Table 693 Meanings of values

Value	Meaning
1	POTS voice entity
2	VoIP voice entity

Table 693 Meanings of values

Value	Meaning
3	VoFR voice entity

Description Use the **select-rule type-first** command to configure a rule for voice entity type selection priority.

Use the **undo select-rule type-first** command to remove a rule for voice entity type selection priority.

By default, voice entities are not selected according to their types.

The command is used to configure the sequence of voice entity type selection priority. If different types of voice entities are qualified for a call connection, the system selects a suitable voice entity according to the voice entity type selection priority rule configured by the **select-rule type-first** command. The order of inputting the parameters determines voice entity type priorities. The system selects the first type first, then the second type, and finally the third type.

Related command: **select-rule rule-order** and **select-rule search-stop**.

Example # Configure the system to select VoIP voice entities in the order of VoIP->POTS->VoFR.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] select-rule type-first 2 1 3
```

select-stop

Syntax **select-stop**

undo select-stop

View Voice entity view

Parameter None

Description Use the **select-stop** command to disable the voice entity search function.

Use the **undo select-stop** command to enable the voice entity search function.

By default, the voice entity search function is enabled.

Related command: **select-rule rule-order** and **select-rule type-first**.

Example # Disable the voice entity search function for voice entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] select-stop
```

send-number

Syntax **send-number** { *digit-number* | **all** | **truncate** }

undo send-number

View POTS entity view

Parameter *digit-number*: Number of digits (that are extracted from the end of a number) to be sent, in the range of 0 to 31. It is not greater than the total number of digits of the called number.

all: Sends all digits of a called number.

truncate: Sends a truncated called number.

Description Use the **send-number** command to configure the number sending mode.

Use the **undo send-number** command to restore the default number sending mode.

By default, the **truncate** mode is used.

Note that:

- This command applies to only POTS voice entities. This command is used to control how to send called numbers to PSTN. You can specify to send some digits (defined by the digit-number argument from right to left) or all digits of called numbers. You can also specify to send truncated called numbers, namely, the ending digits of called numbers that match the dot**.**
- Here the dot represents the virtually matched digits. For details, refer to "dot-match" on page 2628 and "match-template" on page 2599.

Related command: **dot-match** and **match-template** on page 2599.

Example # Configure voice entity 10 to send the last six digits of a called number.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] send-number 6
```

substitute (subscriber line view/voice entity view)

Syntax **substitute** { **called** | **calling** } *list-number*

undo substitute { **called** | **calling** }

View POTS/VoIP/VoFR voice view/Subscriber line voice entity view

Parameter **called**: Applies the number substitution rule to a called number.

calling: Applies the number substitution rule to a calling number.

list-number: Serial number of a number substitution rule list configured by using the **number-substitute** command), in the range of 1 to 2147483647.

Description Use the **substitute** command to bind a calling/called number substitution rule list to the voice subscriber line or voice entity.

Use the **undo substitute** command to remove the binding between a calling/called number substitution rule list and the voice subscriber line or voice entity.

By default, no number substitution rule list is bound to a voice subscriber line or voice entity. That is to say, no number substitution is performed.

Before carrying out the this command, you must first use the **number-substitute** *list-number* command to configure a number substitution rule list in voice dial program view, and then use the **rule** command to configure rules for the list.

According to network requirements, you can complete number substitution in the following two ways.

- *Before a voice entity is matched, you can use the **substitute** command in subscriber line view to substitute the calling/called number specific to a subscriber line.*
- *After a voice entity is matched but before a call is initiated, you can use the **substitute** command in voice entity view to substitute a specified calling/called number.*

Related command: **number-substitute** and **rule**.

Example # Apply number substitution rule list 6 to the called number of the voice subscriber line 1/0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line1/0
[Sysname-voice-line1/0] substitute called 6
```

substitute (voice dial program view)

Syntax **substitute** { **incoming-call** | **outgoing-call** } { **called** | **calling** } *list-number*

undo substitute { **incoming-call | outgoing-call** } { **called** | **calling** } { *list-number* | **all** }

View Voice dial program view

Parameter **incoming-call**: Binds the calling/called number of incoming calls to the number substitution rule list.

outgoing-call: Binds the calling/called number of outgoing calls to the number substitution rule list.

called: Applies the number substitution rule to a called number.

calling: Applies the number substitution rule to a calling number.

all: Specifies all number substitution rule lists.

list-number: Serial number of a number substitution rule list configured by using the **number-substitute** command), in the range of 1 to 2147483647.

Description Use the **substitute** command to bind the calling/called number of incoming/outgoing calls to the specified number substitution rule list.

Use the **undo substitute incoming-call** command to remove the binding.

By default, no number substitution rule list is bound. That is to say, no number substitution is performed.

You should follow these rules when using this command:

- At most 32 number substitution rule lists can be bound.
- The system does not stop searching the bound number substitution rule lists in sequence until one rule is applied successfully.

Related command: **number-substitute** and **rule**.

Outgoing and incoming calls are relative to the IP network. Calls originated to the IP network are incoming calls, while those originated from the IP network or PSTN to PSTN are outgoing calls.

Example # Apply number substitution rule list 5 to called numbers of incoming calls.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] substitute incoming-call called 5
```

Apply number substitution rule lists 5, 6, and 8 to called numbers of outgoing calls.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] substitute outgoing-call called 5
[Sysname-voice-dial] substitute outgoing-call called 6
[Sysname-voice-dial] substitute outgoing-call called 8
```

terminator

Syntax **terminator** *character*

undo terminator

View Voice dial program view

Parameter *character*: Dial terminator, which can be any of 0 through 9, pound sign (#), or asterisk (*).

Description Use the **terminator** command to configure a special character as the dial terminator for length-variable telephone numbers.

Use the **undo terminator** command to remove the dial terminator configuration.

By default, no dial terminator is configured.

Related command: **match-template** on page 2599 and timer.

Example # Specify the pound sign (#) as the dial terminator.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] terminator #
```

175 E1 AND T1 CONFIGURATION COMMANDS

ani

Syntax **ani** { **all** | **ka** }

undo ani

View R2 CAS view

Parameter **all**: Specifies the remote end to send the category of the calling party and calling number.

ka: Specifies the remote end to send only the category of the calling party.

Description Use the **ani** command to enable the terminating point to request calling party information (service category and calling number) from the originating point during call connection.

Use the **undo ani** command to disable the terminating point from requesting calling party information from the originating point.

By default, the terminating point does not request calling party information from the originating point during call connection.

- *Configure the local end with this command to support automatic number identification.*
- *This command applies to R2 signaling only.*
- *Normally the **all** keyword is configured. Use the **ka** keyword only when required by the connected switch to prevent call failures.*

Related command: **cas** and **ani-offset**.

Example # Request the remote office to send calling number category and calling number during call connection.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] ani all
```

ani-offset

Syntax **ani-offset** *number*

undo ani-offset

View R2 CAS view

Parameter *number*: Number of digits to be collected, in the range of 1 to10.

Description Use the **ani-offset** command to configure the number of called number digits that need to be collected prior to requesting calling party information.

Use the **undo ani-offset** command to restore the default value.

Before adequate digits are collected, the system will wait for the next digit until the timer expires. During this period, the system does not request calling party information. It does that only after adequate digits are collected.

By default, the number of digits to be collected before the calling party information is 1.

This command applies to R2 signaling only.

Related command: **cas**, timer, **reverse**, and **renew**.

Example # Start requesting calling number or caller identifier after receiving three digits.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] ani all
[Sysname-cas1/0:0] ani-offset 3
```

answer enable

Syntax **answer enable**

undo answer enable

View R2 CAS view

Parameter None

Description Use the **answer enable** command to configure the originating point to require the terminating point to send answer signal. Only after receiving an answer signal can the two parties begin to talk.

Use the **undo answer enable** command to restore the default.

By default, the originating party requires the terminating party to send answer signal.

This command applies to R2 signaling only.

The R2 line signaling coding schemes in some countries do not include answer signal sending. To accommodate to such schemes, you must configure the **answer enable** command on the originating point. This allows the terminating point to set up calls after a specified time period.

Related command: **re-answer enable** and **timer dl re-answer**.

Example # Configure the originating point to disable the terminating point from sending answer signals.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] undo answer enable
```

callmode

Syntax **callmode** { **segment** | **terminal** }

undo callmode

View R2 CAS view

Parameter **segment**: Specifies the connection mode for an R2 call as segment-to-segment.

terminal: Specifies the connection mode for an R2 call as terminal-to-terminal.

Description Use the **callmode** command to configure the connection mode for an R2 call.

Use the **undo callmode** command to restore the default setting.

By default, the connection mode for an R2 call is **terminal**.

Example # Set the connection mode for an R2 call to **segment**.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas 1/0:0] callmode segment
```

cas

Syntax **cas** *ts-set-number*

View E1/T1 interface view

Parameter *ts-set-number*: Number of a created timeslot (TS) group, in the range of 0 to 30. The number of a T1 timeslot group ranges from 0 to 23.

Description Use the **cas** command to enter R2 CAS view, digital E&M signaling view, or digital LGS signaling view.

After entering a signaling view, you may configure signaling parameters as desired. When doing that, assign the same value to the *ts-set-number* keyword in commands **cas** and **timeslot-set**.

Related command: **timeslot-set**, **ani-offset**, **reverse**, **select-mode**, timer, **trunk-direction**, and **renew**.

Example # Enter the R2 CAS view of TS group 5.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 5
```

clear-forward-ack enable

Syntax **clear-forward-ack enable**

undo clear-forward-ack enable

View R2 CAS view

Parameter None

Description Use the **clear-forward-ack enable** command to enable the terminating point to respond with a clear-back signal when the originating point (the calling party) disconnects a call.

Use the **undo clear-forward-ack enable** command to disable the terminating point to respond with a clear-back signal when the originating point (the calling party) disconnects a call.

By default, the terminating point does not send clear-back signals to acknowledge clear-forward signals.

This command applies to R2 signaling only.

In some countries, if the terminating point controls trunk circuit reset in the R2 signaling exchange process, when the calling party disconnects a call and the originating point sends a clear-forward signal to the terminating point, the terminating point sends a clear-back signal as an acknowledgement, and then sends a release guard signal to indicate that the line of the terminating point is thoroughly released.

During R2 line signaling exchange, trunk circuit reset is sometimes controlled by the called party (terminating point). The practice in some countries in this case is that after the terminating point receives a clear-forward signal from the originating point, it sends back a clear-back signal as an acknowledgement and then a release-guard signal to indicate that the line at the terminating point side is fully released.

Related command: **mode**.

Example # Enable the terminating point to acknowledge clear-forward signals with clear-back signals.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] clear-forward-ack enable
```

display voice subscriber line

Syntax **display voice subscriber line** *slot-number*:{ *ts-set-number* | **15** | **23** }

View Any view

Parameter *slot-number*: Number of the voice subscriber line automatically created upon creation of a TS group or ISDN PRI set.

ts-set-number: Number of the TS group that has been created.

15: Indicates the subscriber line is created on an E1 interface.

23: Indicates the subscriber line is created on a T1 interface.

Description Use the **display voice subscriber line** command to display subscriber line configuration about voice subscriber line description, echo canceller, echo cancellation sampling time length, comfortable noise and so on.

This command applies to both E1 and T1 voice.

Example # Display the configuration of voice subscriber line 5/0:0.

```
<Sysname> display voice subscriber-line 5/0:0
  Current information  -----  subscriber-line5/0:0
    Type                       = R2
    Status                     = PhysicalDown
    Call Status :
        TS  1                  = IDLE
        TS  2                  = IDLE
        TS  3                  = IDLE
        TS  4                  = IDLE
        TS  5                  = IDLE
        TS  6                  = IDLE
        TS  7                  = IDLE
```

```
        TS  8                   = IDLE
        TS  9                   = IDLE
        TS 10                   = IDLE
        TS 11                   = IDLE
        TS 12                   = IDLE
        TS 13                   = IDLE
        TS 14                   = IDLE
        TS 15                   = IDLE
        TS 17                   = IDLE
        TS 18                   = IDLE
    Description                 = subscriber-line5/0:0 Interface
    Private Line                = None
    Cng                         = Enable
    Echo Canceller              = Enable
    Echo Canceller Tail-Length  = 32
    Nlp On                      = Enable
    Fax Detect Mode             = CNG/CED
    Ring Generate               = Enable
    Receive Gain                = 0.0
    Transmit Gain               = 0.0
    DTMF Threshold Digital      = Insensitivty
    PCM Type                    = A-Law
```

Table 694 Description on fields of the display voice subscriber line command

Field	Description
Current information	Information about the current voice subscriber line
Type	Signaling type on the voice subscriber line
Status	Status of the voice subscriber line
Call Status	Status of the voice protocol call
Description	Information about the voice subscriber line
Private Line	Private line dialup mode of the voice subscriber line
Cng	Comfort noise setting on the voice subscriber line
The subscriber line's description	The description of the subscriber line
Echo Canceller	Echo cancellation setting on the voice subscriber line
Echo Canceller Tail-Length	Echo interval setting on the voice subscriber line
Nlp-on	Setting of nonlinear processing (NLP) in the echo canceller on the voice subscriber line
Fax Detect Mode	Fax tone detection mode on the voice subscriber line
Ring Generate	Ringback tone on the voice subscriber line
Receive Gain	Input gain of the voice subscriber line
Transmit Gain	Output gain of the voice subscriber line
DTMF Threshold Digital	DTMF parameters of the digital voice subscriber line
PCM Type	Companding law used for signal quantization on the voice subscriber line

dl-bits

Syntax **dl-bits** { **answer** | **blocking** | **clear-back** | **clear-forward** | **idle** | **seize** | **seizure-ack** | **release-guard** } { **received** | **transmit** } *ABCD*

undo dl-bits { **answer** | **blocking** | **clear-back** | **clear-forward** | **idle** | **seize** | **seizure-ack** | **release-guard** } { **received** | **transmit** }

View R2 CAS view

Parameter **answer**: Answer signal of R2 line signaling.

blocking: Blocking signal of R2 line signaling.

clear-back: Clear-back signal of R2 line signaling.

clear-forward: Clear-forward signal of R2 line signaling.

idle: Idle signal of R2 line signaling.

seize: Seizure signal of R2 line signaling.

seizure-ack: Seizure acknowledgement signal of R2 line signaling.

release-guard: Release guard signal of R2 line signaling.

received: Indicates that the signaling setting applies to received R2 line signals.

transmit: Indicates that the signaling setting applies to transmitted R2 line signals.

ABCD: ABCD bit pattern of R2 line signaling, in the range of 0000 to 1111.

Table 695 Default values of signals in R2 digital line signaling

Signal	Default rx-bits ABCD	Default tx-bits ABCD
Answer	0101	0101
Blocking	1101	1101
Clear-back	1101	1101
Clear-forward	1001	1001
Idle	1001	1001
Seize	0001	0001
Seizure-ack	1101	1101
Release-guard	1001	1001

Description Use the **dl-bits** command to configure the ABCD bit pattern for R2 signals.

Use the **undo dl-bits** command to restore the defaults.

This command applies to R2 signaling only.

You may need to use this command to accommodate to the ABCD bit pattern schemes used in different countries.

When you modify the ABCD bit pattern of a signal, you need to modify the ABCD bit pattern of other signals accordingly so that the whole signaling system can work normally.

Related command: **seizure-ack enable** and **answer enable**.

Example # Set the ABCD bit pattern for received R2 idle signal to 1101, and to 1011 for transmitted R2 idle signal.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] dl-bits idle received 1101
[Sysname-cas1/0:0] dl-bits idle transmit 1011
```

dtmf enable

Syntax **dtmf enable**

undo dtmf enable

View R2 CAS view

Parameter None

Description Use the **dtmf enable** command to set the way receiving and transmitting R2 signals to DTMF mode.

Use the **undo dtmf enable** command to restore the default.

By default, multifrequency compelled (MFC) mode is adopted.

This command applies to R2 signaling only.

Related command: **timer dtmf**.

Example # Adopt DTMF mode to receive and send R2 signals.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] dtmf enable
```

dtmf threshold digital

Syntax **dtmf threshold digital** *value*

undo dtmf threshold digital

View Voice subscriber line view

Parameter **digital**: Sets a digital voice subscriber line.

value: 0 or 1. 0 indicates that DTMF detection is sensitive while "1" indicates that DTMF detection is insensitive.

Description Use the **dtmf threshold digital** command to set the DTMF detection sensitivity.

Use the **undo dtmf threshold digital** command to restore the default DTMF detection sensitivity.

By default, the DTMF detection is insensitive.

The more sensitive the DTMF detection is, the larger the tolerance of DTMF collection is. The possibility of detecting error codes becomes relatively high while the possibility of missing detecting error codes becomes low.

Example # Set the DTMF detection to be insensitive.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscirber-line1/0:0
[Sysname-voice-line1/0:0] dtmf threshold digital 1
```

final-callednum enable

Syntax **final-callednum enable**

undo final-callednum enable

View R2 CAS view

Parameter None

Description Use the **final-callednum enable** command to enable the originating point to send a number terminator to the terminating point after it sends all digits of a called number. After the terminating point receives this terminator, it stops requesting the called number.

Use the **undo final-callednum enable** command to disable the originating point to send a number terminator to the terminating point after it sends all digits of a called number.

By default, no number terminator is sent.

This command applies to R2 signaling only.

You may configure the **final-callednum** command to accommodate to the R2 interregister signaling in some countries where a number terminator can be sent to indicate that all digits of a called number has been sent.

Related command: **register-value digital-end**.

Example # Enable the originating point to send the number terminator signal.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] final-callednum enable
```

force-metering enable

Syntax **force-metering enable**

undo force-metering enable

View R2 CAS view

Parameter None

Description Use the **force-metering enable** command to enable R2 metering signal processing.

Use the **undo force-metering enable** command to disable R2 metering signal processing.

By default, R2 metering signal processing is disabled.

This command applies to R2 signaling only.

When the terminating point supports metering signals, the system may send a forced release signal instead of a clear-back signal to release the line. This is to avoid collision between the clear-back signal sent by the called party and the metering signal.

Example # Enable R2 metering signal processing.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] force-metering enable
```

group-b enable

Syntax **group-b enable**

undo group-b enable

View R2 CAS view

Parameter None

Description Use the **group-b enable** command to enable R2 signaling to use Group B signals to complete registers exchange.

Use the **undo group-b enable** command to disable R2 signaling from using Group B signals to complete registers exchange.

By default, Group B signals are used to complete registers exchange.

This command applies to R2 signaling only.

You may need to configure the **undo** form of this command to accommodate to the R2 interregister signaling in some countries where Group B signals is not supported or cannot be interpreted correctly.

Related command: **register-value req-switch-groupb**.

Example # Adopt Group B signals to complete registers exchange.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] group-b enable
```

line

Syntax **line** *slot-number*:{ *ts-set-number* | **15** | **23** }

undo line

View POTS voice entity view

Parameter *slot-number:* Number of the E1/T1 interface corresponding to a subscriber line.

ts-set-number: Number of the TS group created on the E1/T1 interface.

15: Indicates that the POTS voice entity is to be associated with an E1 voice ISDN PRI interface.

23: Indicates that the POTS voice entity is to be associated with a T1 voice ISDN PRI interface.

Description Use the **line** command to configure the binding between a POTS entity and a logical voice subscriber line.

Use the **undo line** command to remove the binding.

By default, there is no binding between a POTS entity and a logical voice subscriber line.

This command applies to both E1 and T1 voice.

After configuring a target match template with the **match-template** command for a voice entity, you need to associate the entity with a logical interface to indicate from which interface the traffic destined for the target should be routed.

Related command: **timeslot-set**, **entity** on page 2594, and **pri-set**.

Example # Associate a POTS entity with a TS group on an E1 interface.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] line 1/0:1
```

mode

Syntax **mode** *zone-name* [**default-standard**]

undo mode

View R2 CAS view

Parameter *zone-name*: Country or region name. The argument can one of the following values:

- **argentina**: Uses Argentinean R2 signaling standard.
- **australia**: Uses Australian R2 signaling standard.
- **bengal**: Uses Bengalee R2 signaling standard.
- **brazil**: Uses Brazilian R2 signaling standard.
- **china**: Uses Chinese R2 signaling standard.
- **custom**: Uses customized R2 signaling standard.
- **hongkong**: Uses Hongkong R2 signaling standard.
- **india**: Uses Indian R2 signaling standard.
- **indonesia**: Uses Indonesian R2 signaling standard.
- **itu-t**: Uses ITU-T R2 signaling standard.
- **korea**: Uses Korean R2 signaling standard.
- **malaysia**: Uses Malaysian R2 signaling standard.
- **mexico**: Uses Mexican R2 signaling standard.
- **newzealand**: Uses New Zealand R2 signaling standard.
- **singapore**: Uses Singaporean R2 signaling standard.
- **thailand**: Uses Thai R2 signaling standard.

default-standard: Initializes R2 signaling parameters such as values of the **force-metering** command based on national R2 signaling variants.

Description Use the **mode** command to configure a national R2 signaling variant.

Use the **undo mode** command to restore the default.

By default, ITU-T R2 signaling applies.

This command applies to R2 signaling only.

The R2 signaling standards implemented in different countries and regions may vary. They are called ITU variants. To accommodate to the R2 signaling in a country or region, you may use the **mode** command. The system can automatically select the appropriate subscriber line state, service category, metering signal, and signal values of C and D bits, and so on.

At present, the device supports Brazil, Mexico, Argentina, India, New Zealand, Thailand, Bengal, South Korea, Hongkong, Indonesia, and other ITU-T variants.

With the **default-standard** keyword configured, the system initializes the subscriber line status, service type, metering signal and C and D signaling bits and other parameters depending on the default settings of configured national R2 signaling variants.

If the **custom** keyword is configured, you can customize specific signaling exchange procedures and signal values in R2 signaling to accommodate to countries.

Related command: **register-value** and **force-metering enable**.

Example # Adopt Hongkong default R2 signaling.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] mode hongkong default-standard
```

pcm

Syntax **pcm** { **a-law** | **µ-law** }

undo pcm

View Voice subscriber line view

Parameter **a-law**: Companding A-law, used in most part of the world other than North America and Japan, such as China, Europe, Africa, and South America.

µ-law: Companding µ-law, used in North America and Japan.

Description Use the **pcm** command to configure a companding law used for quantizing signals.

Use the **undo pcm** command to restore the default.

Companding laws are adopted to quantize signals unevenly for the purpose of reducing noise and improving signal-to-noise ratio. Underpinning this approach are the statistics about voice signals, which indicate that lower power signals are more likely present than high power signals.

According to CCITT, when devices in two countries use different companding schemes to communicate, the side using μ-law is responsible for converting signals to A-law.

By default, the companding law for VE1 interfaces is A-law, while that for VT1 interfaces is μ-law.

Example # Adopt μ-law companding for signal quantization.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscirber-line1/0:0
[Sysname-voice-line1/0:0] pcm u-law
```

pri-set

Syntax **pri-set** [**timeslot-list** *range*]

undo pri-set

View E1/T1 interface view

Parameter *range*: Specifies timeslots to be bound. Timeslots are numbered 1 through 31 on an E1 interface and 1 to 24 on a T1 interface. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1***-***number2*, or several discrete timeslots by specifying *number1*, *number2***-***number3*. When the range argument is not specified, only TS15 is bound.

Description Use the **pri-set** command to bind timeslots on an E1 or T1 interface into a PRI set.

Use the **undo pri-set** command to remove the timeslot binding.

By default, no PRI set is created.

When creating a PRI set on a CE1/PRI interface, note the following:

- TS0 is used for frame synchronization control (FSC), TS16 as a D channel for signaling transmission, and other timeslots as B channels for data transmission. You may bind the timeslots except for timeslot 0 into a PRI set (as the D channel, timeslot 16 is automatically bundled). This PRI set is logically equivalent to an ISDN PRI interface in the form of 30B + D. If no timeslot is specified, all timeslots except for TS0 are bound into an interface similar to an ISDN PRI interface in the form of 30B+D.
- For the created PRI set, the system automatically creates a serial interface named **serial** *number***:15**.

When creating a PRI set on a T1 interface, note the following:

- TS24 is used as D channel for signaling transmission, and other timeslots as B channels for data transmission. You may randomly bind these timeslots into a PRI set (as the D channel, TS24 is automatically bound). This PRI set is logically equivalent to an ISDN PRI interface in the form of 23B + D.
- For the created PRI set, the system automatically creates a serial interface named **serial** *number***:23**.

*The **pri-set** command is independent of the DSP resource (voice processing module- VPM). When no DSP resource is available, though IP calls cannot be placed, local TDM calls can still be placed. Therefore, you can configure this command even if no DSP resource is available.*

Example # On interface E1 1/0 bind timeslots 1, 2, and 8 through 12 into a PRI set.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] pri-set timeslot-list 1,2,8-12
```

re-answer enable

Syntax **re-answer enable**

undo re-answer enable

View R2 CAS view

Parameter None

Description Use the **re-answer** command to enable the originating point to support re-answer signal processing.

Use the **undo re-answer enable** command to restore the default.

By default, the originating point does not support re-answer signal processing.

This command applies to R2 signaling only.

In some countries, re-answer process is needed in R2 signaling. When the terminating point sends a clear-back signal, the originating point does not release the line right away, but maintains the call state instead. If it receives the re-answer signal from the terminating point within a specified time, it continues the call; otherwise, it disconnects the call upon timeout.

Related command: **answer enable** and **timer dl re-answer**.

Example # Enable the originating point to process re-answer signals.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
```

```
[Sysname-e1 1/0] cas 0
[Sysname-cas 1/0:0] re-answer enable
```

register-value

Syntax **register-value** { **billingcategory** | **callcreate-in-groupa** | **callingcategory** | **congestion** | **demand-refused** | **digit-end** | **nullnum** | **req-billingcategory** | **req-callednum-and-switchgroupa** | **req-callingcategory** | **req-currentcallednum-in-groupc** | **req-currentdigit** | **req- firstcallednum-in-groupc** | **req-firstcallingnum** | **req-firstdigit** | **req-lastfirstdigit** | **req-lastseconddigit** | **req-lastthirddigit** | **req-nextcallednum** | **req-nextcallingnum** | **req-switch-groupb** | **subscriber-abnormal** |**subscriber-busy** | **subscriber-charge** |**subscriber-idle** } *value*

undo register-value { **billingcategory** | **callcreate-in-groupa** | **callingcategory** | **congestion** | **demand-refused** | **digit-end** | **nullnum** | **req-billingcategory** | **req-callednum-and-switchgroupa** | **req-callingcategory** | **req-currentcallednum-in-groupc** | **req-currentdigit** | **req- firstcallednum-in-groupc** | **req-firstcallingnum** | **req-firstdigit** | **req-nextcallednum** | **req-nextcallingnum** | **req-lastfirstdigit** | **req-lastseconddigit** | **req-lastthirddigit** | **req-nextcallednum** | **req-nextcallingnum** | **req-specialsignal** | **req-switch-groupb** | **subscriber-abnormal** |**subscriber-busy** | **subscriber-charge** |**subscriber-idle** }

View R2 CAS view

Parameter **billingcategory** *value*: Specifies the billing category value, in the range 1 to 16. It configures the KA signal in R2 signaling. The KA signal is sent by the originating point forward to the originating toll office or originating international exchange to indicate calling category. The signal provides two types of information for this call connection: billing category (regular, immediate, or toll free) and subscriber level (with or without priority).

callcreate-in-groupa *value:* Specifies the direct call setup signal value, in the range 1 to 16.

callingcategory *value*: Specifies the calling category signal value, in the range 1 to 16. It configures the R2 KD signal. It functions to identify whether break-in and forced- release can be implemented by or on the calling party.

congestion *value*: Specifies the congestion signal value, in the range 1 to 16.

demand-refused *value*: Specifies the request-refused signal value, in the range 1 to 16.

digit-end *value*: Specifies the digit-end signal value, in the range 1 to 16.

nullnum *value*: Specifies the null number signal value, in the range 1 to 16.

req-billingcategory *value*: Specifies the send billing category signal value, in the range 1 to 16.

req-callednum-and-switchgroupa *value*: Specifies the send last digit and changeover to Group A signal value, in the range 1 to 16.

req-callingcategory *value*: Specifies the send calling category signal value, in the range 1 to 16.

req-currentcallednum-in-groupc *value*: Specifies the send current called number signal in Group C state, in the range 1 to 16.

req-currentdigit *value*: Specifies the send current digit signal, in the range 1 to 16.

req-firstcallednum-in-groupc *value*: Specifies the send first digit signal value in Group C state, in the range 1 to 16.

req-firstcallingnum *value*: Specifies the send calling number signal value, in the range 1 to 16.

req-firstdigit *value*: Specifies the send first digit signal value, in the range 1 to 16.

req-lastfirstdigit *value*: Specifies the send last digit signal value, in the range 1 to 16.

req-lastseconddigit *value*: Specifies the send last second digits signal value, in the range 1 to 16.

req-lastthirddigit *value*: Specifies the send last three digits signal value, in the range 1 to 16.

req-nextcallednum *value*: Specifies the send next called number signal value, in the range 1 to 16.

req-nextcallingnum *value*: Specifies the send next calling number signal value, in the range 1 to 16.

req-switch-groupb *value*: Specifies the changeover to Group B signal value, in the range 1 to 16.

subscriber-abnormal *value*: Specifies the subscriber's line abnormal signal value, in the range 1 to 16.

subscriber-busy *value*: Specifies the subscriber's line busy signal value, in the range 1 to 16.

subscriber-idle *value*: Specifies the subscriber's line idle value, in the range 1 to 16. It configures the R2 KB signal used for describing the called subscriber's line status, for example, whether the line is idle. It acknowledges and controls call connection. If your router is connected to a PBX, change the KB value on the router to that used on the PBX, in case different KB values are used. If your router is connected to another router, you only need to make sure that the same KB signal value is used between them.

The defaults vary by national variant.

Description Use the **register-value** command to configure R2 register signal values.

Use the **undo register-value** command to restore the defaults.

You may set a signal value to 16 to indicate that the signal function does not exist. For example, if the send last digit signal is not available in a national R2 signaling variant, you may set the value for **req-lastfirstdigit** to 16.

The purpose of the **register-value** command is to assign values for signals requesting responses from the remote end. For example, after you configure the **register-value callingcategory** command, the terminating point sends the send calling category signal with the specified value to the originating point for the calling category.

This command applies to R2 signaling only.

*As some national register signal coding schemes may not support all the register signals mentioned in this section, you are recommended to use defaults unless necessary. For example, the ITU-T recommendation is available with the send calling category signal (the **callingcategory** keyword) but not the send billing category (**billingcategory**) signal.*

Related command: **group-b enable**.

Example # Request the originating point to send calling category by configuring a backward signal (signal value 7).

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] register-value req-callingcategory 7
```

renew

Syntax **renew** *ABCD*

undo renew

View R2 CAS view

Parameter *ABCD*: Defines the default of each signal bit in transmission. Each bit can take the value of 0 or 1. The default C and D bit values vary by country mode.

Description Use the **renew** command to configure the values of C bit and D bit in R2 signaling.

Use the **undo renew** command to restore the default. The default value varies with R2 signaling standards in countries.

This command applies to R2 signaling only.

R2 signaling uses bits A and B to convey real status information while leaving bits C and D constant. The values of bits C and D are national variant dependent. For example, they are fixed to 01 in most countries but 11 in some other countries.

You may use this command to adapt values of bits C and D to different line signaling coding schemes. The settings of bits A and B in this command however are not necessarily the real ones during transmission.

Related command: **cas** and **reverse**.

Example # Set bits C and D of R2 line signaling to 11.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] renew 0011
```

reverse

Syntax **reverse** *ABCD*

undo reverse

View R2 CAS view

Parameter *ABCD*: Indicates whether corresponding ABCD bits in R2 signaling need inversion. Each argument in this command takes either of the two values: 0 for normal or 1 for inversion. The default is 0000, that is, inversion disabled.

Description Use the **reverse** command to configure line signal inversion mode.

Use the **undo reverse** command to invert ABCD bits of the current line signaling whose values are "1" after the **reverse** command is executed.

This command applies to R2 signaling only.

You may configure an interface to invert the values of any ABCD bits before sending or after receiving a line signal by replacing 0 with 1 or vice versa.

Related command: **cas** and **renew**.

Example # Invert the values of bits B and D in R2 line signaling.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] reverse 0101
```

seizure-ack enable

Syntax **seizure-ack enable**

undo seizure-ack enable

View R2 CAS view

Parameter None

Description Use the **seizure-ack enable** command to configure the originating point to require the terminating point to send seizure acknowledgement signal during R2 line signaling exchange.

Use the **undo seizure-ack enable** command to restore the default.

By default, the originating point requires the terminating point to send seizure acknowledgement signal.

This command applies to R2 signaling only.

Normally, the terminating point acknowledges received seizure signals. The R2 line signaling coding schemes in some countries however do not require the terminating point to do this. To accommodate to these schemes, you can configure the **undo seizure-ack enable** command, allowing the terminating point not to acknowledge received seizure signals.

Related command: **timer dl seizure**.

Example # Disable the terminating point to send seizure acknowledgement signals.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] undo seizure-ack enable
```

select-mode

Syntax **select-mode** [**max** | **maxpoll** | **min** | **minpoll**]

undo select-mode

View CAS view

Parameter **max**: Selects the timeslot with the greatest number from currently available timeslots.

maxpoll: Selects the timeslot with the greatest number from available timeslots in the first timeslot polling; in later pollings, selects in descending order timeslots with numbers less than the one picked out in the previous polling. Suppose TS31 and TS29 are not available. In the first polling, TS30 will be picked out for use and in the next polling, TS28.

min: Selects the timeslot with the lowest number from available timeslots.

min: Selects the timeslot with the smallest number from currently available timeslots.

minpoll: Selects the timeslot with the lowest number from available timeslots in the first timeslot polling; in later pollings, selects in ascending order timeslots with numbers greater than the one picked out in the previous polling. Suppose TS1 and TS3 are not available. In the first polling, TS2 will be picked out for use and in the next polling, TS4.

Description Use the **select-mode** command to set the E1 trunk routing mode.

Use the **undo select-mode** command to restore the default.

By default, the timeslot with the smallest number is selected.

Related command: **cas** and **trunk-direction**.

Example # Set the trunk routing mode for TS group 5 to **max** on interface E1 1/0.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 5
[Sysname-cas1/0:5] select-mode max
```

sendring ringbusy enable

Syntax **sendring ringbusy enable**

undo sendring ringbusy enable

View R2 CAS view

Parameter None

Description Use the **sendring ringbusy enable** command to enable the terminating point to send busy tones to calling subscribers.

Use the **undo sendring ringbusy enable** command to disable the terminating point from sending busy tones to calling subscribers.

By default, the terminating point sends busy tones to calling subscribers.

This command applies to R2 signaling only.

Related command: **timer ring**.

Example # On TS group 5 on interface E1 1/0 configure the terminating point to send ringback tone to the calling side.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 5
[Sysname-cas1/0:5] sendring ringbusy enable
```

signal-value

Syntax **signal-value** { **received idle** | **received seize** | **transmit idle** | **transmit seize** } *ABCD*

undo signal-value { **received idle** | **received seize** | **transmit idle** | **transmit seize** }

View Digital E&M voice subscriber line view

Parameter **received idle**: Indicates the receive idle signal of digital E&M signaling.

received seize: Indicates the receive seized signal of digital E&M signaling.

transmit idle: Indicates the transmit idle signal of digital E&M signaling.

transmit seize: Indicates the transmit seized signal of digital E&M signaling.

ABCD: Default ABCD bit pattern during transmission, with each bit taking the value of 0 or 1.

Description Use the **signal-value** command to configure the ABCD bit patterns of idle receive, receive seized, idle transmit, and transmit seized signals on the digital E&M voice subscriber line.

Use the **undo signal-value** command to restore the defaults.

By default, the ABCD bit patterns of the receive idle signal and the transmit idle signal are 1101, and the ABCD bit patterns of the receive seized signal and the transmit seized signal are 0101. After changing the ABCD bit pattern of a digital E&M signal, you must shut down the digital E&M subscriber line with the **shutdown** command and then bring the line up with the **undo shutdown** command. Otherwise, the voice subscriber line cannot work normally.

Related command: **subscriber line**.

Example # Set the ABCD bit pattern to 1011 for the transmit seized signal on digital E&M subscriber line 1/0:0.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscirber-line1/0:0
[Sysname-voice-line1/0:0] signal-value transmit seize 1011
```

special-character

Syntax **special-character** *character number*

undo special-character *character number*

View R2 CAS view

Parameter *character*: Special character, which can be a pound sign (#) or asterisk (*), A, B, C, or D.

number: Code of register signal, in the range 11 to 16.

Description Use the **special-character** command to configure the special characters acceptable during register signal exchange.

Use the **undo special-character** command to remove the configured special characters.

By default, no special characters are configured.

This command applies to R2 signaling only.

You may need to configure this command to accommodate to some national R2 signaling variants where Group I forward signals can represent special characters such as pound signs (#) and asterisks (*) in addition to digits.

- *You cannot use the **special-character** command to assign a special character different signal values.*
- *To ensure that the device can process calls correctly, assign special characters different signal values.*

Example # Assign the pound sign (#) the register signal code 11.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] special-character # 11
```

subscriber line

Syntax **subscriber line** *slot-number*:{ *ts-set-number* | **15** | **23** }

View Voice view

Parameter *slot-number*: Number of the voice subscriber line automatically created upon creation of a TS group or ISDN PRI set.

ts-set-number: Number of the TS group that has been created.

15: Indicates the subscriber line is created for the ISDN PRI set created on an E1 interface.

23: Indicates the subscriber line is created for the ISDN PRI set created on a T1 interface.

Description Use the **subscriber line** command to enter E1/T1 voice subscriber line view.

Upon creation of a TS group on an E1/T1 interface, the system automatically creates a logical voice subscriber line numbered in the form of *E1/T1 interface number***:***TS group number*. On the voice subscriber line, you can conveniently configure signaling and other voice functions for the corresponding E1/T1 line. Note that on each E1/T1 interface you can create only one TS group.

After you create a PRI set with the **pri-set** command on an E1/T1 interface, a voice subscriber line is automatically created. This line is numbered *E1 interface-number***:15** on an E1 interface and *T1 interface-number***:23** on a T1 interface.

Related command: **timeslot-set** and **pri-set**.

Example # Enter the view of voice subscriber line 1/0:15.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] subscriber-line 1/0:15
[Sysname-voice-line1/0:15]
```

tdm-clock

Syntax **tdm-clock** { **internal** | **line** [**primary**] }

undo tdm-clock

View E1/T1 interface view

Parameter **internal**: Sets the time division multiplexing (TDM) clock source on the E1/T1 interface to internal crystal oscillator TDM clock. The E1/T1 interface thus obtains clock from the crystal oscillator on the mainboard. If it fails to do that, the interface obtains clock from the crystal oscillator on its E1/T1 card. As SIC cards are not available with crystal oscillator clocks, E1/T1 interfaces on SIC cards can only obtain clock from the mainboard. The internal clock source is also referred to as master clock mode in some features.

line: Sets the TDM clock source on the E1/T1 interface to line TDM clock. The E1/T1 interface thus obtains clock from the remote device through the line. The line clock source is also referred to as slave clock mode in some features.

line *primary*: Sets the TDM clock source on the E1/T1 interface to line TDM clock with priority. The E1/T1 interface thus always attempts to use the line TDM clock prior to any other clock sources.

Description Use the **tdm-clock** command to set the TDM clock source for an E1/T1 interface.

Use **undo tdm-clock** command to restore the default.

By default, the TDM clock source for an E1 or T1 interface is the internal clock.

When digital voice E1/T1 interfaces perform TDM timeslot interchange, it is important for them to achieve clock synchronization to prevent frame slips and bit errors.

Depending on your configurations on E1/T1 interfaces, the system adopts different clocking approaches. When there is a subcard VCPM on the mainboard, the clock distribution principle is as follows:

- If the **line** keyword is specified for all interfaces, the clock on the interface with the lowest number is adopted. In case the interface goes down, the clock on the interface with the next lowest number is adopted.
- If the **line primary** keywords are specified for one interface, the clock on the interface is adopted. In one system, you can do this on only one interface.
- If the **line** keyword is specified for one interface and the **internal** keyword for all others, the clock on the interface is adopted.
- Normally, you cannot set the clock source for all interfaces in a system to internal. This is to prevent frame slips and bit errors. You can do this however if the remote E1/T1 interfaces adopt the line clock source.

When there is no VCPM on the mainboard, the configuration of each MIM/FIC is independent but only one interface is allowed to be set to line primary on the same device.

Example # Set the TDM clock source on interface E1 1/0 to line clock.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] tdm-clock line
```

timer dl

Syntax **timer dl** { **answer** | **clear-back** | **clear-forward** | **seizure** | **re-answer** | **release-guard** } *time*

undo timer dl { **answer** | **clear-back** | **clear-forward** | **seizure** | **re-answer** | **release-guard** }

View R2 CAS view

Parameter **answer** *time*: Timeout time in milliseconds of R2 answer signal, in the range of 100 to 120,000 with a default of 60,000. After the originating point sends a seizure acknowledgement signal, the terminating point should send back an answer signal within the timeout time. If the terminating point fails to send an answer signal within the timeout time, the originating point will clear the connection. Timeout time of R2 answer signal should be configured at both the originating point and the terminating point. The timeout time of answer signals from the terminating point is configured at the originating point, while the

timeout time of answer signals for internal function call in a module is configured at the terminating point.

clear-back *time*: Timeout time in milliseconds of R2 clear-back signal, in the range of 100 to 60,000 with a default of .10,000. After the terminating point sends a clear-back signal, it should recognize the forward signal sent back by the originating point within the timeout time.

clear-forward *time*: Timeout time in milliseconds of R2 clear-forward signal configured at the originating point, in the range of 100 to 60,000 with a default of 10,000. After the originating point sends a clear-forward signal, the terminating point should send back a corresponding line signal, clear-back or release guard for example, within the timeout time.

seizure *time* : Timeout time in milliseconds of R2 seizure signal configured at the originating point, in the range of 100 to 5,000 with a default of 1,000. After the originating point sends a seizure signal, the terminating point should send back a seizure acknowledgement signal within the timeout time.

re-answer *time*: Timeout time in milliseconds of R2 re-answer signal configured at the originating point, in the range 100 to 60,000 milliseconds with a default of 1,000. The originating point releases the line if it does not receive another answer signal from the terminating point after it recognizes the clear-back signal.

release-guard *time*: Timeout time in milliseconds of R2 release guard signal configured at the originating point, in the range of 100 to 60,000 with a default of 1,000. The originating point should send a release guard signal within the timeout time after it receives a clear-back signal from the terminating point in response to a clear-forward signal.

Description Use the **timer dl** command to configure timeouts of R2 line signals.

Use the **undo timer dl** command to restore the defaults.

This command applies to R2 signaling only.

Example # Set the timeout time of R2 seizure signal to 300 milliseconds.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] timer dl seize 300
```

timer dtmf

Syntax **timer dtmf** *time*

undo timer dtmf

View R2 CAS view

Parameter *time*: Delay before sending a DTMF signal in milliseconds, in the range of 50 to 10,000.

Description Use the **timer dtmf** command to configure the delay from when the originating point receives a seizure acknowledgement signal to when it starts sending DTMF signals.

Use the **undo timer dtmf** command to restore the default.

By default, the delay is 50 milliseconds.

This command applies to R2 signaling only.

Normally, the originating point starts sending DTMF signals immediately after receiving a line seizure acknowledgement signal. Sometimes, however, you may need to introduce a delay to accommodate to the digit collection process on the remote PBX.

Related command: **dtmf enable**.

*Before you can configure this command, you must configure the **dtmf enable** command.*

Example # Configure the R2 signaling to start sending DTMF signals 800 milliseconds later after receiving a seizure acknowledgement signal.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] dtmf enable
[Sysname-cas1/0:0] timer dtmf 800
```

timer register-pulse persistence

Syntax **timer register-pulse persistence** *time*

undo timer register-pulse persistence

View R2 CAS view

Parameter **persistence** *time*: Duration in milliseconds of R2 register pulse signals, in the range of 50 to 3,000.

Description Use the **timer register-pulse persistence** command to configure the duration of R2 register pulse signals such as A-3, A-4, and A-6.

Use the **undo timer register-pulse persistence** command to restore the default, that is, 150 milliseconds.

By default, the duration is 150 milliseconds.

This command applies to R2 signaling only.

When the terminating point sends a backward register pulse signal, A-3 for example, the signal must persist for a specified time period. When the originating point receives the signal, it sends back a Group II forward signal. When the originating point recognizes the pulse signal, A4, A6, or A15, it stops sending any forward signal, and terminates the register signal exchange.

Related command: **timer register-complete group-b**.

Example # Set the duration of R2 register pulse signals to 300 milliseconds.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] timer register-pulse persistence 300
```

timer register-complete group-b

Syntax **timer register-complete group-b** *time*

undo timer register-complete group-b

View R2 CAS view

Parameter **group-b** *time*: Maximum time in milliseconds that the originating point waits for R2 Group B signals, in the range of 100 to 90,000.

Description Use the **timer register-complete group-b** command to configure the timeout value of R2 group B signals. After the terminating point switch to Group B, it should send Group B signals within this time period.

Use the **undo timer register-complete** command to restore the default timeout value of R2 group B signals.

By default, the maximum time is 30,000 milliseconds.

This command applies to R2 signaling only.

Related command: **timer dl**.

Example # Configure the maximum Group B signal exchange time to 10,000 milliseconds.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] timer register-complete group-b 10000
```

timer ring

Syntax **timer ring** { **ringback** | **ringbusy** } *time*

undo timer ring { **ringback** | **ringbusy** }

View R2 CAS view

Parameter **ringback** *time*: Sets the duration in milliseconds of playing ringback tone, in the range of 1,000 to 90,000.

ringbusy *time*: Sets the duration in milliseconds of playing busy tone, in the range of 1,000 to 90,000.

Description Use the **timer ring** command to configure the duration of playing a signal tone when R2 signaling is adopted.

Use the **undo timer ring** command to restore the default duration of playing a signal tone.

By default, the duration of playing the ringback tone is 60,000 milliseconds and that of playing the busy tone is 30,000 milliseconds.

This command applies to R2 signaling only.

Related command: **send-ring** on page 2608.

Example # Set the duration of playing the ringback tone to 10,000 milliseconds when R2 signaling is adopted.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 0 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 0
[Sysname-cas1/0:0] timer ring ringback 10000
```

timeslot-set

Syntax **timeslot-set** *ts-set-number* **timeslot-list** *timeslots-list* **signal** { **e&m-delay** | **e&m-immediate** | **e&m-wink** | **fxo-ground** | **fxo-loop** | **fxs-ground** | **fxs-loop** | **r2** }

undo timeslot-set *ts-set-number*

View E1/T1 interface view

Parameter *ts-set-number*: TS group number. For an E1 interface, the TS group number ranges from 0 to 30, and for a T1 interface, the TS group number ranges from 0 to 23.

timeslots-list: Timeslot range. Timeslots are numbered 1 through 31 for an E1 interface and 1 through 24 for a T1 interface. TS 16 for an E1 interface (or TS24 for a T1 interface) is used to transmit control signaling.

signal: Specifies a signaling mode for the TS group, which should be consistent with that adopted by the central office. It includes the following types of signaling:

- **e&m-delay**: Adopts the delay start mode of digital E&M signaling.
- **e&m-immediate**: Adopts the immediate start mode of digital E&M signaling.
- **e&m-wink**: Adopts the wink start mode of digital E&M signaling.
- **fxo-ground**: Adopts the FXO ground start mode of digital LGS signaling.
- **fxo-loop**: Adopts the FXO loop start mode of digital LGS signaling.
- **fxs-ground**: Adopts the FXS ground start mode of digital LGS signaling.
- **fxs-loop**: Adopts the FXS loop start mode of digital LGS signaling.
- **r2**: Adopts ITU-T Q.421 R2 digital line signaling. This is the one most commonly used.

Description Use the **timeslot-set** command to create a TS group and specify a signaling mode for it on the E1/T1 interface.

Use the **undo timeslot-set** command to remove the TS group.

By default, no TS group is configured.

Only after you create a TS group can you use the **subscriber-line** command to enter subscriber line view to configure voice-related attributes.

Related command: **subscriber line** and **cas**.

*The **timeslot-set** command is independent of the DSP resource (voice processing module, VPM). When no DSP resource is available, though IP calls cannot be placed, local TDM calls can still be placed. Therefore, you can configure this command even if no DSP resource is available.*

Example # Create TS group 5, including TS1 through TS31 and using R2 signaling.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
```

trunk-direction

Syntax **trunk-direction timeslots** *timeslots-list* { **dual** | **in** | **out** }

undo trunk-direction timeslots *timeslots-list*

View R2 CAS view

Parameter *timeslots-list*: Timeslot range. Timeslots are numbered 1 through 31 on an E1 interface and 1 through 24 on a T1 interface. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1*-*number2*, or several discrete timeslots by specifying *number1*, *number2*-*number3*. Examples are 1-14, 15, 17-31.

dual: Bidirectional trunk.

in: Incoming trunk.

out: Outgoing trunk.

Description Use the **trunk-direction** command to configure the R2 signal trunking direction.

Use the **undo trunk-direction** command to restore the default.

By default, bidirectional trunking applies.

This command applies to R2 signaling only.

An incoming trunk carries incoming calls but not outgoing calls while the outgoing trunk does the contrary. A bidirectional trunk carries both incoming calls and outgoing calls.

For R2 signaling to operate normally for call connection, you need to ensure that the trunking mode is incoming at one end of the trunk and outgoing at the other end. If both ends are using bidirectional trunking mode, use the **select-mode** command to tune trunking policy. This is to prevent timeslot contention.

In addition, avoid using bidirectional trunking mode at one end and outgoing mode at the other end, because this can lead to failures of outgoing calls at the end in bidirectional trunking mode.

Related command: **cas** and **select-mode**.

Example # Set the trunking mode to bidirectional for TS group 5 on interface E1 1/0.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 5
[Sysname-cas1/0:5] trunk-direction timeslots 1-31 dual
```

---

ts

Syntax **ts** { **block** | **open** | **query** | **reset** } **timeslots** *timeslots-list*

View CAS view

Parameter **block**: Blocks the trunk circuit of specified timeslots to make it unavailable.

open: Opens the trunk circuit of specified timeslots, allowing it to carry services.

query: Queries status of the trunk circuit of specified timeslots to see whether the circuit is busy, open, or blocked in real time.

reset: Resets the trunk circuit of specified timeslots when it cannot automatically reset. You may need to do this if the state of an administratively blocked or opened circuit cannot recover for example.

timeslots *timeslots-list*: Specifies a timeslot range. Timeslots are numbered 1 through 31 on for an E1 interface and 1 through 24 for a T1 interface. You may specify a single timeslot by specifying a number, a range of timeslots by specifying a range in the form of *number1***-***number2*, or several discrete timeslots by specifying *number1*, *number2***-***number3*. Examples are 1-14, 15, 17-31.

Description Use the **ts** command to maintain the trunk circuit of specified timeslots.

*The **ts query** command is available in R2 CAS view, digital E&M CAS view, and digital LGS CAS view.*

Related command: **cas**.

Example # Reset the circuit of timeslots 1 through 15 in TS5 and query the status of the circuit of TS1 through TS31.

```
<Sysname> system-view
[Sysname] controller e1 1/0
[Sysname-e1 1/0] timeslot-set 5 timeslot-list 1-31 signal r2
[Sysname-e1 1/0] cas 5
[Sysname-cas1/0:5] ts reset timeslots 1-15
[Sysname-cas1/0:5] ts query timeslots 1-31
```

176 FAX OVER IP CONFIGURATION COMMANDS

default entity fax

Syntax **default entity fax baudrate** { **2400** | **4800** | **9600** | **14400** | **disable** | **voice** }

default entity fax ecm

default entity fax level *level*

default entity fax local-train threshold *threshold*

default entity fax nsf-on

default entity fax protocol { **standard-t38 | t38** } [**hb-redundancy** *number* | **lb-redundancy** *number*]

default entity fax protocol pcm { **g711alaw** | **g711ulaw** }

default entity fax train-mode { **local** | **ppp** }

undo default entity fax { **baudrate** | **ecm** | **level** | **local-train threshold** | **nsf-on** | **protocol** | **train-mode** }

View Voice dial program view

Parameter **baudrate**: Specifies the maximum transmission rate of the fax. The default value is **voice**.

- **2400**: Sets the maximum transmission rate to 2400 bps.
- **4800**: Negotiates the baud rate first in accordance with the V.27 fax protocol. The maximum transmission rate is 4800 bps.
- **9600**: Negotiates the baud rate first in accordance with the V.29 fax protocol. The maximum transmission rate to 9600 bps.
- **14400**: Negotiates the baud rate first in accordance with the V.17 fax protocol. The maximum transmission rate to 14400 bps.
- **disable**: Disables the fax forwarding capability.
- **voice**: Sets the fax rate to the allowed maximum voice speed for different codec protocols.

ecm: Enables the fax error correction mode. It is disabled by default.

level *level*: Specifies the fax signal level in dBm (in the range of -60 to -3). The default value is -15.

local-train threshold *threshold*: Specifies the threshold percentage of fax local training (in the range of 0 to 100). The default value is 10.

nsf-on: Enables NSF message transmission. It is disabled by default.

protocol: Specifies the transport protocol of the fax. By default, the T.38 fax protocol is applied. Both **hb-redundancy** *number* and **lb-redundancy** *number* default to 0.

- **standard-t38**: Adopts the standard T.38 (UDP) fax protocol, which supports H.323-T.38 and SIP-T.38 protocols.
- **pcm**: Enables the passthrough mode.
- **g711alaw**: Adopts G.711 A-law.
- **g711ulaw**: Adopts G.711 μ-law.
- **t38**: Enables T.38 fax protocol.
- **hb-redundancy** *number*: Number of redundant high-speed T.38 packets, in the range of 0 to 2.
- **lb-redundancy** *number*: Number of redundant low-speed T.38 packets, in the range of 0 to 5.

train-mode: Specifies the fax training mode. By default, the point-to-point training mode is adopted.

- **local**: Adopts local training.
- **ppp**: Adopts point-to-point training.

Description Use the **default entity fax** command to set fax parameters to the default values globally.

Use the **undo default entity fax** command to restore the fax parameters of the system to the defaults.

*You must carry out the **default entity fax train-mode local** command before the configuration made by the **default entity fax local-train threshold** command takes effect.*

Example # Set the maximum fax rate to 9,600 bps globally.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] default entity fax baudrate 9600
```

display voice fax

Syntax **display voice fax statistics**

View Any view

Parameter None

Description Use the **display voice fax statistics** command to view the FoIP statistics.

Example # Display the FoIP statistics.

```
<Sysname> display voice fax statistics

  Statistics about Fax Session:
  {
    Total :  0
    FAX_VOFR_STANDARD_SWITCH:  0
    FAX_VOFR_FRF11_TRUNK    :  0
    FAX_VOFR_FRF11_SWITCH   :  0
    FAX_VOFR_MOTOROLA       :  0
    FAX_VOIP_STDT38         :  0
    FAX_VOIP_T38            :  0

    Success :  0
    FAX_VOFR_STANDARD_SWITCH:  0
    FAX_VOFR_FRF11_TRUNK    :  0
    FAX_VOFR_FRF11_SWITCH   :  0
    FAX_VOFR_MOTOROLA       :  0
    FAX_VOIP_STDT38         :  0
    FAX_VOIP_T38            :  0

    Failure :  0
    FAX_VOFR_STANDARD_SWITCH:  0
    FAX_VOFR_FRF11_TRUNK    :  0
    FAX_VOFR_FRF11_SWITCH   :  0
    FAX_VOFR_MOTOROLA       :  0
    FAX_VOIP_STDT38         :  0
    FAX_VOIP_T38            :  0

    Last Time :  00:00:00
    FAX_VOFR_STANDARD_SWITCH:  00:00:00
    FAX_VOFR_FRF11_TRUNK    :  00:00:00
    FAX_VOFR_FRF11_SWITCH   :  00:00:00
    FAX_VOFR_MOTOROLA       :  00:00:00
    FAX_VOIP_STDT38         :  00:00:00
    FAX_VOIP_T38            :  00:00:00

    Processed Pages :  0
    FAX_VOFR_STANDARD_SWITCH:  0
    FAX_VOFR_FRF11_TRUNK    :  0
    FAX_VOFR_FRF11_SWITCH   :  0
    FAX_VOFR_MOTOROLA       :  0
    FAX_VOIP_STDT38         :  0
    FAX_VOIP_T38            :  0
  }

  Statistics about using fax baudrate:
  {
    V27 2400 :  0
    V27 4800 :  0
    V29 7200 :  0
    V29 9600 :  0
    V17 7200 :  0
    V17 9600 :  0
    V17 12000:  0
    V17 14400:  0
  }

  Statistics about using ECM or Non-ECM mode:
  {
```

```
  ECM    :  0
  Non-ECM:  0
}

Statistics about release reason:
{
  WAIT_DP_BEG_DEMODULATE_TIMEOUT :  0
  WAIT_DP_BEG_MODULATE_TIMEOUT   :  0
  WAIT_DP_END_DEMODULATE_TIMEOUT :  0
  WAIT_DP_END_MODULATE_TIMEOUT   :  0
  WAIT_FRAMEACK_TIMEOUT          :  0
  WAIT_T30MSG_PSTN_TIMEOUT       :  0
  WAIT_T30MSG_IP_TIMEOUT         :  0
  SPOOL_TIME_OVER                :  0
  GET_INVALID_T30MESSAGE         :  0
  IPP_CALL_RELEASE               :  0
  NORMAL_RELEASE                 :  0
  UNKNOWN_REASON                 :  0
}
```

Table 696 Description on fields of the display voice fax statistics command

Field	Description
FAX_VOFR_STANDARD_SWITCH	Fax statistics for standard VoFR
FAX_VOFR_FRF11_TRUNK	Fax statistics for FRF.11 trunk VoFR
FAX_VOFR_FRF11_SWITCH	Fax statistics for FRF.11 switched VoFR
FAX_VOFR_MOTOROLA	Fax statistics for Motorola compatible VoFR
FAX_VOIP_STDT38	Fax statistics for standard T.38 VoIP
FAX_VOIP_T38	Fax statistics for T.38 VoIP
WAIT_DP_BEG_DEMODULATE_TIMEOUT	Statistics of the number of connections released in the case that the DP does not start demodulation within the specified time
WAIT_DP_BEG_MODULATE_TIMEOUT	Statistics of the number of connections released in the case that the DP does not start modulation within the specified time
WAIT_DP_END_DEMODULATE_TIMEOUT	Statistics of the number of connections released in the case that the DP does stop demodulation within the specified time
WAIT_DP_END_MODULATE_TIMEOUT	Statistics of the number of connections released in the case that the DP does not stop modulation within the specified time
WAIT_FRAMEACK_TIMEOUT	Statistics of the number of connections released in the case that no Frame ACK message is received from the DP within the specified time
WAIT_T30MSG_PSTN_TIMEOUT	Statistics of the number of connections released in the case that no T.30 message is received from PSTN within the specified time
WAIT_T30MSG_IP_TIMEOUT	Statistics of the number of connections released in the case that no T.30 message is received from the IP network within the specified time

Table 696 Description on fields of the display voice fax statistics command

Field	Description
SPOOL_TIME_OVER	Statistics of the number of connections released in the case that the number of spooling attempts exceeds the maximum
GET_INVALID_T30MESSAGE	Statistics of the number of connections released owing to invalid T.30 message
IPP_CALL_RELEASE	Statistics of the number of released IPP calls
NORMAL_RELEASE	Statistics of the number of connections released normally
UNKNOWN_REASON	Statistics of the number of connections released for unknown reasons

fax baudrate

Syntax **fax baudrate { 2400 | 4800 | 9600 | 14400 | disable | voice }**

undo fax baudrate

View POTS/VoIP/VoFR entity view

Parameter **2400:** Sets the maximum fax baud rate to 2,400 bps.

4800: Negotiates the fax baud rate first in accordance with the V.27 fax protocol. The maximum fax baud rate is 4,800 bps.

9600: Negotiates the fax baud rate first in accordance with the V.29 fax protocol. The maximum fax baud rate is 9,600 bps.

14400: Negotiates the fax baud rate first in accordance with the V.17 fax protocol. The maximum fax baud rate is 9,600 bps.

disable: Disables the fax function.

voice: Finalizes the allowed maximum fax baud rate first in accordance with voice encoding/decoding protocols.

- If G.711 is adopted, the fax baud rate is 14,400 bps and the fax protocol is V.17.
- If G.723.1 Annex A is adopted, the fax baud rate is 4,800 bps and the fax protocol is V.27.
- If G.726 is adopted, the fax baud rate is 14,400 bps and the fax protocol is V.17.
- If G.729 is adopted, the fax baud rate is 9,600 bps and the fax protocol is V.29.

Description Use the **fax baudrate** command to configure the maximum fax baud rate.

Use the **undo fax baudrate** command to restore the default maximum fax baud rate.

Note that if the baud rate is set to a value other than "**disable**" and "**voice**", the rate is negotiated first in accordance with the corresponding fax protocol. Here the rate refers to the allowed maximum rate, instead of the actual rate.

Example # Configure the gateway to negotiate the fax rate in accordance with the V.29 fax protocol.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 4 pots
[Sysname-voice-dial-entity4] fax baudrate 9600
```

fax ecm

Syntax **fax ecm**

undo fax ecm

View POTS/VoIP entity view

Parameter None

Description Use the **fax ecm** command to configure the gateway to use the ECM mode by force.

Use the **undo fax ecm** command to restore the default.

By default, the ECM mode is not used on the gateway.

The **fax ecm** command is used to perform the forced restriction on the gateway. If the facsimile terminals at both ends support the ECM mode, but the non-ECM mode has been configured on the gateway side, then the non-ECM mode is selected. If either or both of the facsimile terminals do not support the ECM mode, the non-ECM mode is selected. Only when the facsimile terminals on both sides support the ECM mode and the gateway uses the ECM mode, the ECM mode will be selected.

You must enable the ECM mode for the POTS and VoIP entities of the fax sender and receiver in the ECM mode.

Example # Configure the gateway to adopt the ECM mode by force.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 4 pots
[Sysname-voice-dial-entity4] fax ecm
```

fax level

Syntax **fax level** *level*

undo fax level

View POTS/VoIP/VoFR entity view

Parameter *level:* Level of the energy transmitted by a gateway carrier in dBm, in the range of -60 to -3. The greater the value is, the higher the energy is. The smaller the value is, the higher the attenuation is.

Description Use the **fax level** command to configure the transmit energy level of a gateway carrier.

Use the **undo fax level** command to restore the default.

By default, the transmit energy level of a gateway carrier is -15 dBm.

Usually the default transmit energy level of a gateway carrier is acceptable. If fax still cannot be sent when other configurations are correct, try to adjust the transmit energy level.

Example # Set the transmit energy level of the gateway carrier to -20 dBm.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 4 pots
[Sysname-voice-dial-entity4] fax level -20
```

fax local-train threshold

Syntax **fax local-train threshold** *threshold*

undo fax local-train threshold

View POTS/VoIP/VoFR entity view

Parameter *threshold:* Fax local training threshold in percentages, in the range of 0 to 100.

Description Use the **fax local-train threshold** command to configure the fax local training threshold.

Use the **undo fax local-train threshold** command to restore the default.

By default, the fax local training threshold is 10.

The point-to-point training means that the gateway does not participate in the rate training between two facsimile terminals. In this mode, rate training is

performed between two facsimile terminals and is transparent to the gateways. Therefore, for the point-to-point training, the gateway does not participate in rate training and the threshold is invalid.

*When the local training mode is adopted, the local training threshold configured with the **fax local-train threshold** command is valid. When the PPP training mode is adopted, the gateway does not participate in the rate training and the local training threshold is invalid.*

Example # Configure the fax local training threshold to 20.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] fax train-mode local
[Sysname-voice-dial-entity10] fax local-train threshold 20
```

fax nsf-on

Syntax **fax nsf-on**

undo fax nsf-on

View POTS/VoIP entity view

Parameter None

Description Use the **fax nsf-on** common to configure the signal transmission mode of fax capability as a nonstandard mode.

Use the **undo fax nsf-on** command to restore the default transmission mode.

By default, the standard signal transmission mode of fax capability is adopted.

In some cases such as encrypted fax, both facsimile terminals adopt a nonstandard faculty (NSF) to negotiate. At the start of negotiation, both terminals first exchange NSF message frames, and then negotiate the subsequent fax capability for communication. NSF messages are standard T.30 messages and carry private information.

In order to use NSF for negotiation, the following conditions must be satisfied:

- Fax terminals must support nonstandard transmission mode.
- The signal transmission mode of the fax capability must be set to a nonstandard mode in the POTS and VoIP entities for both the fax terminals.

Example # Configure NSF for fax signal transmission.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
```

```
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] fax nsf-on
```

fax protocol

Syntax **fax protocol** { **t38** | **standard-t38** } [**hb-redundancy** *number* | **lb-redundancy** *number*]

fax protocol pcm { **g711alaw** | **g711μlaw** }

undo fax protocol

View POTS/VoIP entity view

Parameter **t38**: Uses T.38 fax protocol. With this protocol, a fax connection can be set up quickly.

standard-t38: Uses the standard T38 protocol, which supports H.323 and SIP.

lb-redundancy *number*: Indicates the number of low-speed redundant packets. The *number* argument ranges from 0 to 5, and defaults to 0.

hb-redundancy *number*: Indicates the number of high-speed redundant packets. The *number* argument ranges from 0 to 2, and defaults to 0.

pcm: Enables the transparent transmission in the passthrough mode.

g711alaw: Enables G.711 A-law.

g711ulaw: Enables G.711 μ-law.

Description Use the **fax protocol** command to configure the type of protocol used for fax communication with other devices.

Use the **undo fax protocol** command to restore the default type of protocol used for fax communication with other devices.

With the T.38 protocol adopted, if the call adopts H.323, the fax will use the standard T.38 negotiation mode stipulated by the H.323; if the call adopts SIP, the fax will use the standard T.38 negotiation mode stipulated by SIP.

By default, T.38 negotiation mode is used for fax.

- Low-speed data refers to the V.21 command data, while high-speed data refers to the TCF and image data.
- To communicate with leading fax terminals in the industry, the standard T.38 protocol must be selected. Likewise, to communicate with other fax terminals supporting a T.38 protocol, the T.38 protocol must be adopted. As the leading devices do not support local training mode for fax, the point-to-point training mode must be adopted in order to implement interworking with the leading devices in the industry.

- Increasing the number of redundant packets will improve reliability of network transmission and reduce packet loss ratio. A great amount of redundant packets, however, can increase bandwidth consumption to a great extent and thereby, in the case of low bandwidth, affect the fax quality seriously. Therefore, the number of redundant packets should be selected properly according to the network bandwidth.
- The passthrough mode is subject to such factors as loss of packet, jitter and delay, so the clock on both communication sides must be kept synchronized. At present, only G.711 A-law and G.711 m-law are supported, and the voice activity detection (VAD) function should be disabled.

Example # Set to 2 the number of high-speed redundant packets sent via the T.38 fax protocol.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 4 pots
[Sysname-voice-dial-entity4] fax protocol t38 hb-redundancy 2
```

fax train-mode

Syntax **fax train-mode** { **local** | **ppp** }

undo fax train-mode

View POTS/VoIP/VoFR entity view

Parameter **local**: Adopts the local training mode.

ppp: Adopts the point-to-point protocol (ppp) training mode.

Description Use the **fax train-mode** command to configure the fax training mode.

Use the **undo fax train-mode** command to restore the default.

By default, the PPP training mode is adopted.

VoFR entities only support the PPP training mode.

Example # Configure the local training mode for the gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 pots
[Sysname-voice-dial-entity10] fax train-mode local
```

reset voice fax statistics

Syntax **reset voice fax statistics**

View User view

Parameter None

Description Use the **reset voice fax statistics** command to clear FoIP statistics.

Example # Clear FoIP statistics.

```
<Sysname> reset voice fax statistics
```

voip h323-conf tcs-t38

Syntax **voip h323-conf tcs-t38**

undo voip h323-conf tcs-t38

View Voice view

Parameter None

Description Use the **voip h323-conf tcs-t38** command to enable the voice gateway in H.323 slow-start mode to contain the T.38 capability description in its capability set.

Use the **undo voip h323-conf tcs-t38** command to disable the voice gateway in H.323 slow-start mode from containing the T.38 capability description in its capability set.

By default, T.38 capability description is contained.

Because NetMeeting does not support T.38 capability description parsing, you must disable the voice gateway in H.323 slow-start mode from containing the T.38 capability description in its capability set to interwork with NetMeeting.

- *This command has global significance. The execution of this command can enable all voice entities to contain the T.38 capability description in their capability sets.*
- *Because NetMeeting does not support T.38 capability description parsing, you must configure the **voip h323-conf tcs-t38** command before interworking with NetMeeting.*
- *If interworking with NetMeeting is required for a voice entity, you can disable fax using the **fax baudrate disable** command or set the fax mode to a non-T.38 mode (**pcm**).*

Example # Disable the voice gateway in H.323 slow-start mode from containing T.38 capability description in its capability set.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] undo voip h323-conf tcs-t38
```

177 H.323 CONFIGURATION COMMANDS

area-id

Syntax **area-id** *string*

undo area-id [*string*]

View Gatekeeper client view

Parameter *string*: Area ID, a digit string that is 1 to 31 characters in length. The pound signs (#) can be used as delimiters in the string.

Description Use the **area-id** command to assign an area ID to the H.323 gateway.

Use the **undo-area-id** command to remove the specified or all area IDs.

By default, no area ID is assigned to the H.323 gateway.

Each area ID identifies a particular type of gateway, for example, 1# for the voice gateway and 2# for the video gateway, depending on the agreement that the gateway and the gatekeeper reaches beforehand. When a VoIP entity communicates with the gatekeeper, the gatekeeper uses the received area ID to identify the type of the gateway.

You may assign up to 30 area IDs to the H.323 gateway.

Related command: **match-template** on page 2599, **entity** on page 2594.

Example # Assign area ID 6# to the gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] area-id 6#
```

display voice gateway

Syntax **display voice gateway**

View Any view

Parameter None

Description Use the **display voice gateway** command to display the registration state information of the voice gateway, such as the registration state, gateway alias, and local telephone number list of the gateway.

Example # Display the registration state information of the voice gateway.

```
<Sysname> display voice gateway
  GW_Status = Registered
  GK_ID     = GhostLand
  Current GW information:
    H323-ID    1962
    E164-ID    1119
    E164-ID    100
    E164-ID    400
    E164-ID    1234
    E164-ID    07552001
    E164-ID    07552002
    E164-ID    660019

  Current GK information:
    H323-ID    1962
    E164-ID    1119
    E164-ID    100
    E164-ID    400
    E164-ID    1234
    E164-ID    07552001
    E164-ID    07552002
    E164-ID    660019
```

Table 697 Description on the fields of the display voice gateway command

Field	Description
GW_Status	Registration state of the gateway
GK_ID	ID of the gatekeeper with which the gateway is registered
Current GW information: H323-ID	H323 ID of the gateway
Current GW information: E164-ID	E.164 number on the gateway
Current GK Information: H323-ID	H.323 ID registered on the gatekeeper for the gateway
Current GK Information: E164-ID	E.164 numbers registered on the gatekeeper for the gateway

gk-client

Syntax **gk-client**

View Voice view

Parameter None

Description Use the **gk-client** command to enter gatekeeper client view to configure voice and gatekeeper parameters.

Use the **quit** command to exit this view.

Related command: **area-id**, **gk-2nd-id**, **gk-id**, **gw-address**, **gw-id**, and **ras-on**.

Example # Enter gatekeeper client view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk]
```

gk-2nd-id

Syntax **gk-2nd-id** *gk-name* **gk-addr** *gk-ipaddress* [*ras-port*]

undo gk-2nd-id

View Gatekeeper client view

Parameter *gk-name*: Gatekeeper name, a string of 1 to 128 case sensitive characters.

gk-ipaddress: IP address of gatekeeper.

ras-port: RAS port used by the gatekeeper, an integer in the range 1 to 65535. The default is 1719.

Description Use the **gk-2nd-id** command to configure the secondary gatekeeper for the gateway.

Use the **undo gk-2nd-id** command to remove the secondary gatekeeper.

By default, no secondary gatekeeper is specified for the gateway.

For reliability sake, a backup mechanism is provided for gatekeepers. In case the communication with a primary gatekeeper is abnormal (for example, timeout occurs) or the primary gatekeeper becomes unavailable, gateways can turn to a secondary gatekeeper for registration.

*Before you can configure a secondary gatekeeper, you must first configure a primary gatekeeper with the **gk-id** command.*

Related command: **gk-id**.

Example # Configure a secondary gatekeeper, setting its IP address to 1.1.1.2, name to gk-backup, and RAS port to the default.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
```

```
[Sysname-voice-gk] gk-id gk-center gk-addr 1.1.1.1
[Sysname-voice-gk] gk-2nd-id gk-backup gk-addr 1.1.1.2
```

gk-id

Syntax **gk-id** *gk-name* **gk-addr** *gk-ipaddress* [*ras-port*]

undo gk-id

View Gatekeeper client view

Parameter *gk-name*: Gatekeeper name, a string of 1 to 128 case sensitive characters.

gk-ipaddress: IP address of gatekeeper.

ras-port: RAS port used by the gatekeeper, an integer in the range 1 to 65535. The default is 1719.

Description Use the **gk-id** command to configure the primary gatekeeper for the gateway.

Use the **undo gk-id** command to remove the primary gatekeeper.

By default, no primary gatekeeper is specified for the gateway.

Only after you configure the information of the primary gatekeeper can the gateway locate the gatekeeper for registration.

Related command: **area-id**, **gw-id**, **gk-2nd-id**, **gw-address**, **ras-on**.

Example # Configure the primary server, setting its IP address to 1.1.1.1, name to gk-center, and RAS port to the default.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] gk-id gk-center gk-addr 1.1.1.1
```

gk-security call enable

Syntax **gk-security call enable**

undo gk-security call enable

View Gatekeeper client view

Parameter None

Description Use the **gk-security call enable** command to enable security calling on the voice gateway.

Use the **undo gk-security call enable** command to disable security calling on the voice gateway.

By default, security calling is enabled.

CAUTION: *Disable security calling for the voice gateway if the called gatekeeper cannot handle call tokens.*

Example # Disable security calling for the voice gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] undo gk-security call enable
```

gk-security register-pwd

Syntax **gk-security register-pwd** { **cipher** | **simple** } *password*

undo gk-security register-pwd

View Gatekeeper client view

Parameter **cipher**: Displays passwords in ciphertext.

simple: Displays passwords in plain text.

password: A string of 1 to 16 characters excluding spaces.

Description Use the **gk security register-pwd** command to configure a password for registration with the gatekeeper.

Use the **undo gk-security register-pwd** command to remove the registration password.

By default, no registration password is configured on the voice gateway.

Note that messages exchanged during the entire registration process will carry the registration password, if it is configured on the voice gateway.

Example # Configure a registration password **aaa** and set its display mode to **ciphertext**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] gk-security register-pwd cipher aaa
```

gw-address

Syntax **gw-address** *ip-address*

undo gw-address

View Gatekeeper client view

Parameter *ip-address*: Source IP address to be bound to the voice gateway.

Description Use the **gw-address** command to bind a source IP address with the voice gateway.

Use the **undo gw-address** command to remove the binding.

By default, no source IP address is bound to the voice gateway.

CAUTION:

- *Use this command before configuring the **ras-on** command. In case the latter has been configured, undo it first.*
- *To make calls successfully, ensure that the source IP address is a valid IP address already assigned to an Ethernet or loopback interface on the device, and in addition, this address and the address of the peer H.323 entity (a gatekeeper, terminal, or MCU) are reachable to each other.*

Related command: **area-id**, **gk-2nd-id**, **gk-id**, **gw-address**, and **ras-on**.

Example # Bind the source IP address 1.1.1.1 to the voice gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] gw-address 1.1.1.1
```

gw-id

Syntax **gw-id** *namestring*

undo gw-id

View Gatekeeper client view

Parameter *namestring*: Gateway alias (gateway identifier), a string of 1 to 128 case-sensitive characters.

Description Use the **gw-id** command to assign an alias to the gateway. This alias overwrites the old one, if any.

Use the **undo gw-id** command to remove the alias.

By default, no alias is assigned to the gateway.

Note that each gateway can be assigned only one alias. It is used by the gatekeeper to identify the gateway.

Related command: **area-id**, **gk-2nd-id**, **gk-id**, **gw-address**, and **ras-on**.

Example # Assign the alias citya-gw to the gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] gw-id citya-gw
```

ras-on

Syntax **ras-on**

undo ras-on

View Gatekeeper client view

Parameter None

Description Use the **ras-on** command to activate gatekeeper client to register with the gatekeeper.

Use the **undo ras-on** command to deactivate gatekeeper client.

By default, the gatekeeper client is disabled.

Only when the gatekeeper client function is active can the normal communication be maintained between the voice gateway and the gatekeeper. When the function is inactive, the voice gateway cannot set up connection with the gatekeeper.

The GK client can be enabled only after the GK- and gateway-related configurations are completed.

Related command: **gw-id**, **gw-address**, and **gk-id**.

Example # Activate gatekeeper client.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] gk-client
[Sysname-voice-gk] gw-id gateway1
[Sysname-voice-gk] gw-address 192.168.1.1
[Sysname-voice-gk] gk-id gatekeeper gk-addr 192.168.1.2
[Sysname-voice-gk] ras-on
```

voip h323-descriptor

Syntax **voip h323-descriptor** *descriptor*

undo voip h323-descriptor

View Voice view

Parameter *descriptor:* H.323 descriptor, comprising 1 to 64 characters.

Description Use the **voip h323-descriptor** command to configure an H.323 descriptor for the voice gateway.

Use the **undo voip h323-descriptor** command to restore the default H.323 descriptor.

By default, the descriptor is **Wqldg0Hcwfydz**.

You are recommended to use the default descriptor.

If at both ends are the devices of H3C, you are recommended to configure the same descriptor for them.

Example # Configure an H.323 descriptor **mystring** for the voice gateway.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] voip h323-descriptor mystring
```

178 SIP CONFIGURATION COMMANDS

display voice sip call-statistics

Syntax **display voice sip call-statistics**

View Any view

Parameter None

Description Use the **display voice sip call-statistics** command to display the statistics about all SIP calls.

Example # Display the statistics about all SIP calls.

```
<Sysname> display voice sip call-statistics
Message Statistics of Stack:


TPT Message                 UDP   TCP   SCTP  TLS   Total
------------------------------------------------------------------

InMsg                        0      0      0      0      0
OutMsgSucc                  0      0      0      0      0
OutMsgFail                  0      0      0      0      0

TXN Message                 Inv_Cli NonInv_Cli Inv_Srv NonInv_Srv

------------------------------------------------------------------

Create Succ                    0          0          0          0
Create Fail                    0          0          0          0
Terminal Abnom                0          0          0          0

Request Message   Inv  Ack  Bye  Can  Opt  Reg  Inf  Prk Upd
------------------------------------------------------------------
  In:                0    0    0    0    0    0    0    0    0
 Out:                0    0    0    0    0    0    0    0    0

Response Message                1xx  2xx  3xx  4xx  5xx  6xx
------------------------------------------------------------------
  In:                             0    0    0    0    0    0
 Out:                             0    0    0    0    0    0

Error Statistics:
--------------------------------------
       callCb creation failures:     0
     call-leg creation failures:     0
  transaction creation failures:    0
         callCb locate failures:      0
       call-leg locate failures:      0
```

```
    transaction locate failures:     0
            user not registered:       0
             user not available:       0
   request with missing headers:     0
 response-no To tag in response:     0
         response - invalid via:       0
  messages without headers rcvd:     0
            SDP decode failures:       0
          registration timeouts:       0
retransmitted requests received:     0
           transaction timeouts:       0
```

Table 698 Description on fields of the display voice sip call-statistics command

Field	Description
TPT Message	Statistics about SIP transport layer messages, including UDP, TCP, SCTP, and TLS. The messages of each type fall into InMsg, (received), OutMsgSucc (transmitted successfully), and OutMsgFail (sending failure).
TXN Message	Statistics of SIP transaction messages. These messages fall into: ■ Inv_Cli (Invite transaction of client) ■ NonInv _Cli (Non-invite transaction of client) ■ Inv_Srv (Invite transaction of server) ■ NonInv _Srv (Non-invite transaction of server) Each type of message can be displayed by: ■ Create Succ (Creation success) ■ Create Fail (Creation failure) ■ Terminal Abnom (Terminal exception)
Request Message	Statistics of all SIP request messages, including Inv (Invite), Ack, Bye, Can (Cancel), Opt (Option), Reg (Register), Inf (Information), Prk (Prack), Upd (Update) Each type of message can be displayed by: ■ In (received) ■ Out (sent)
Response Message	Statistics of all SIP response messages, including 1XX, 2XX, 3XX, 4XX (Cancel), 5XX and 6XX Each type of message can be displayed by: ■ In (received) ■ Out (sent)
callCb creation failures	Statistics of call control block creation failures in SIP
call-leg creation failures	Statistics of call leg creation failures in SIP
transaction creation failures	Statistics of transaction creation failures in SIP
callCb locate failures	Statistics of call control block location failures in SIP
call-leg locate failures	Statistics of call leg location failures in SIP
transaction locate failures	Statistics of transaction location failures in SIP
user not registered	Statistics of user not registered message in SIP
user not available	Statistics of user not available message in SIP
request with missing headers	Statistics of request messages with missing headers in SIP
response-no To tag in response	Statistics of response messages without the To Tag field in SIP

Table 698 Description on fields of the display voice sip call-statistics command

Field	Description
response - invalid via	Statistics of response messages with an invalid via field in SIP
messages without headers rcvd	Statistics of received messages without headers in SIP
SDP decode failures	Statistics of SDP decoding failures in SIP
registration timeouts	Statistics of registration timeouts in SIP
retransmitted requests received	Statistics of received transmission requests in SIP
transaction timeouts	Statistics of transaction timeouts in SIP

display voice sip register-state

Syntax **display voice sip register-state**

View Any view

Parameter None

Description Use the **display voice sip register-state** command to display status information of all user numbers to be registered on the SIP UA.

Example # Display all registration status information on the SIP UA.

```
<Sysname> display voice sip register-state
Number                    Entity     Registrar Address     Expires Status
+-------------------------------------------------------------------------+
105                       105        100.1.1.1:5060        30      login
2000                      107        100.1.1.1:5060        200     online
```

Table 699 Description on fields of the display voice sip register status command

Field	Description
Number	User number
Entity	Entity number
Registrar Address	Address of the registrar, in the format of IP address + port number
Expires	Aging time for a user number in seconds
Status	State in which a number stays, including: ■ offline ■ online ■ login ■ logout

outband sip

Syntax **outband sip**

undo outband

View POTS/VoIP entity view

Parameter None

Description Use the **outband sip** command to configure the SIP out-of-band transmission.

Use the **undo outband sip** command to restore the default DTMF transmission mode.

By default, the inband DTMF transmission mode is adopted.

Example # Configure the out-of-band SIP DTMF transmission for VoIP entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 voip
[Sysname-voice-dial-entity10] address sip ip 10.1.1.2
[Sysname-voice-dial-entity10] outband sip
```

proxy

Syntax **proxy ipv4** *ip-address* [**port** *port-number*]

undo proxy ipv4

View SIP client view

Parameter **ipv4** *ip-address*: IPv4 address of the proxy server.

port *port-number*: Port number of the proxy server, in the range of 1 to 65535. The default port number is 5060.

Description Use the **proxy** command to configure proxy server information on the SIP UA.

Use the **undo** proxy command to remove the proxy server information from the SIP UA.

By default, no proxy server information is configured on the SIP UA.

Example # Configure the IP address 169.54.5.10 and port number 1120 for the proxy server.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] proxy ipv4 169.54.5.10 port 1120
```

register-enable

Syntax **register-enable** { **off** | **on** }

undo register-enable

View SIP client view

Parameter **off**: Disables the SIP registration function.

on: Enables the SIP registration function.

Description Use the **register-enable on** command to enable the SIP registration function.

Use the **register-enable off** command or the **undo register-enable** command to disable the SIP registration function.

By default, the SIP registration function is disabled.

Example # Enable the SIP registration function.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip]sip-server master 169.54.5.10
[Sysname-voice-sip] register-enable on
```

registrar ipv4

Syntax **registrar ipv4** *ip-address* [**port** *port-number*] [**expires** *seconds*] [**slave**]

undo registrar ipv4 [**slave**]

View SIP client view

Parameter *ip-address*: IP address of the registrar.

port *port-number*: Port number of the registrar, in the range of 1 to 65535. The default port number is 5060.

expires *seconds*: Aging time for registration in seconds, in the range of 60 to 65,535. The default aging time is 3,600.

slave: Specifies the registrar as a slave server.

Description Use the **registrar ipv4** command to configure registrar information on the SIP UA.

Use the **undo registrar ipv4** command to remove the registrar information from the SIP UA.

By default, no registrar information is configured on the SIP UA.

You can use this command only when the SIP registration function is disabled.

Example # Configure the IP address 169.54.5.10, the port number 1120, and the aging time 120 seconds for the master registrar.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] registrar ipv4 169.54.5.10 port 1120 expires 120
```

reset voice sip

Syntax **reset voice sip**

View User view

Parameter None

Description Use the **reset voice sip** command to clear all the statistics about the SIP client.

Example # Clear all the statistics about the SIP client.

```
<Router> reset voice sip
```

sip

Syntax **sip**

View Voice view

Parameter None

Description Use the **sip** command to enter SIP client view.

Before you can configure a UA, you should first enter its view with this command.

Example # Enter SIP client view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip]
```

sip-comp

Syntax **sip-comp** { **callee** | **from** }

undo sip-comp { **callee** | **from** }

View SIP client view

Parameter **callee**: Extracts the called number from the To field.

from: Configures the device to use the IP address in the To field as the IP address in the From field when sending a SIP request for interoperability with other vendors. By default, the From field indicates the calling address and the To field indicates the called address.

Description Use the **sip-comp** command to configure SIP compatibility.

Use the **undo sip-comp** command to restore the default SIP compatibility setting.

By default, the SIP compatibility option is not configured.

Example # Configure the device to use the IP address in the To field as the IP address in the From field when sending a SIP request.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-comp from
```

sip-comp agent

Syntax **sip-comp agent** *product-name product-version*

undo sip-comp agent

View SIP client view

Parameter **agent** *product-name product-version*: Indicates the content of the User-Agent header field in SIP request messages. The *product-name* and *product-version* arguments respectively represent the product name and product version of the UAC, each of which is a case-sensitive string of 1 to 31 characters other than { and }.

Description Use the **sip-comp agent** command to configure the User-Agent header field in SIP request messages.

Use the **undo sip-comp agent** command to remove the configuration.

By default, the User-Agent header field in SIP request messages is not configured.

Example Set the User-Agent header field in SIP request messages to company 1.0.

```
<Sysname> system-view
[Sysname] voice-setup
```

```
[Sysname-voice] sip
 [Sysname-voice-sip] sip-comp agent company 1.0
```

sip-comp server

Syntax **sip-comp server** *product-name product-version*

undo sip-comp server

View SIP client view

Parameters **server** *product-name product-version*: Indicates the content of the Server header field in SIP response messages. The *product-name* and *product-version* arguments respectively represent the product name and product version of the UAS, each of which is a case-sensitive string of 1 to 31 characters other than { and }.

Description Use the **sip-comp server** command to configure the Server header field in SIP response messages.

Use the **undo sip-comp server** command to remove the configuration.

By default, the Server header field in SIP response messages is not configured.

Examples Set the Server header field in SIP response messages to company 1.1.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-comp server company 1.1
```

sip-domain

Syntax **sip-domain** *domain-name*

undo sip-domain

View SIP client view

Parameter *domain-name*: Domain name of the SIP server, comprising 1 to 31 characters, which can be 0 through 9, A through Z or a through z, underscore "_", hyphen "-", and period ".".

Description Use the **sip-domain** command to configure the domain name of a SIP device.

Use the **undo sip-domain** command to remove the domain name setting of the SIP device.

SIP addresses can be domain name addresses or IP addresses. As IP addresses of devices are more likely to change, domain name addresses are preferred where fixed SIP addresses are desired.

By default, IP address is used.

Example # Set the domain name of the SIP device to hello.com.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] sip-domain hello.com
```

source-ip

Syntax **source-ip** *ip-address*

undo source-ip

View SIP client view

Parameter *ip-address*: IPv4 address.

Description Use the **source-ip** command to configure the source IP address bound to the packets sent by the UA.

Use the **undo source-ip** command to remove the configuration.

By default, no source IP address is configured to be bound to the packets sent by the UA.

Note that the source IP address must be already assigned to a gateway interface.

You can use this command only when the SIP registration function is disabled.

Example # Specify 1.1.1.1 as the source IP address bound to the packets sent by the UA.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] source-ip 1.1.1.1
```

user

Syntax **user** *username* **password** { **cipher** | **simple** } *password* [**cnonce** *cnonce* | **realm** *realm*] *****

undo user

View SIP client view/POTS entity view

Parameter *username*: Username used for registration authentication, a string of 1 to 31 case-sensitive characters. The characters " " " and " " are invalid.

cipher: Displays the password of the current user in cipher text.

simple: Displays the password of the current user in plain text.

password: Password used for authentication, a case-sensitive string of 1 to 16 characters or 24 characters. When you specify the **cipher** keyword but enter a password in plain text mode or when specify the **simple** keyword, the password may contain 1 to 16 characters. When you specify the **cipher** keyword and enter a password in cipher text mode, the password must contain 24 characters.

cnonce *cnonce*: Authentication information field used for handshake authentication between the SIP server and the SIP UA, This field consists of a string of 1 to 50 case-sensitive characters. The characters " " " and " " are invalid.

realm *realm*: Domain name used for handshake authentication between the SIP server and SIP UA. The domain name consists of a string of 1 to 50 case-sensitive characters. The characters " " " and " " are invalid.

Description Use the **user** command to configure SIP authentication information.

Use the **undo user** command to restore the default.

By default, the username and password in SIP client view are VOICE-GATEWAY and VOICE-SIP, respectively, while no SIP authentication information is configured in POTS entity view.

CAUTION:

- *If realm is configured on the SIP UA, ensure that the value is the same as that configured on the server. Otherwise, the SIP UA will fail the authentication due to mismatch. If realm is not configured on a SIP UA, the SIP UA will perform no realm match and consider that the value of realm configured on the server is trusted.*
- *If it is necessary to configure authentication information in POTS entity view, the same authentication information is recommended for the POTS entities configured with the same telephone number.*
- *In the case of authentication, it is forbidden to execute the **user** command after the registration function is enabled because this operation may result in registration update failures.*

Example Configure global SIP authentication information as follows:

- Username: abcd
- Password: 1234
- Display mode: cipher

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] user abcd password cipher 1234
```

wildcard-register enable

Syntax **wildcard-register enable**

undo wildcard-register

View SIP client view

Parameter None

Description Use the **wildcard-register enable** command to enable fuzzy (wildcard) telephone number registration.

Use the **undo wildcard-register** command to disable fuzzy (wildcard) telephone number registration.

By default, fuzzy telephone number registration is disabled.

When configuring a match template in a POTS entity, you may use a number containing the wildcards of dot (.) and T instead of using a standard E.164 number. After enabling fuzzy telephone number registration, the router retains the wildcard "." and substitutes the asterisk ***** for the wildcard T when sending REGISTER messages.

You can use this command only when the SIP registration function is disabled.

You may use fuzzy telephone number registration only when it is supported on both SIP SIP server and location server.

Example # Enable fuzzy telephone number registration.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] sip
[Sysname-voice-sip] wildcard-register enable
```

179 VoFR Configuration Commands

address

Syntax **address** { **vofr-dynamic serial** *interface-number dlci-number* | **vofr-static serial** *interface-number dlci-number cid-number* }

undo address { **vofr-dynamic** | **vofr-static** }

View VoFR entity view

Parameter **vofr-dynamic**: Specifies a VoFR entity to adopt the dynamic call mode.

vofr-static: Specifies a VoFR entity to adopt the FRF.11 trunk mode.

serial *interface-number*: Specifies the destination interface of a VoFR entity.

dlci-number: Destination virtual circuit number of a VoFR entity, in the range of 16 to 1007.

cid-number: Destination FRF.11 sub-channel number of a VoFR entity, in the range of 4 to 255.

Description Use the **address** command to configure a channel to the peer voice gateway.

Use the **undo address** command to remove the configuration.

By default, no channel to the peer voice gateway is configured.

Note that:

- The FRF.11 sub-channel number to be configured must be available. That is, the FRF.11 sub-channel is not occupied.
- A voice channel will be established for the VoFR entity immediately you execute the **address vofr-static** command. The voice channel will be removed after you execute the undo form of the command or delete the VoFR entity.

Related command: **call-mode**, **vofr**, **trunk-id**, and **display fr vofr-info**.

Example # Specify DLCI 100 to adopt the dynamic call mode.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
```

```
[Sysname-voice-dial] entity 4 vofr
[Sysname-voice-dial-entity4] match-template 12345
[Sysname-voice-dial-entity4] address vofr-dynamic serial1/0 100
```

call-mode

Syntax **call-mode** { **dynamic** | **static** }

undo call-mode

View VoFR entity view

Parameter **dynamic**: Adopts the dynamic call mode.

static: Adopts the FRF.11 trunk mode.

Description Use the **call-mode** command to configure the mode in which calls between the VoFR entity and the peer voice entity are established.

Use the **undo call-mode** command to restore the default call mode.

By default, the dynamic mode is adopted.

- *Dynamic call mode: When a call is originated, the frame relay will randomly select an idle FRF.11 sub-channel to establish a voice channel. After the call is completed, the frame relay will immediately remove the voice channel and release the corresponding FRF.11 sub-channel. The call control protocol used in the dynamic call mode is specified by executing the **vofr** command in interface DLCI view.*
- *FRF.11 trunk mode: A voice channel is established when you execute the **address vofr-static** command. The voice channel is directly used to establish calls. After the call is completed, the voice channel remains until it is manually cleared. In the FRF.11 trunk mode, you must use the **trunk-id** command to configure a PSTN-dialed number for the terminating VoFR entity.*

Related command: **trunk-id** and **address**.

Example # Configure the FRF,11 trunk mode for VoFR entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 vofr
[Sysname-voice-dial-entity10] call-mode static
```

cid select-mode

Syntax **cid select-mode** { **max-poll** | **min-poll** }

undo cid select-mode

View Interface DLCI view

Parameter **max-poll**: Selects circuit IDs cyclically in descending order

min-poll: Selects circuit IDs cyclically in ascending order

Description Use the **cid select-mode** command to configure the CID selection mode which the originating side of a VoFR call adopts.

Use the **undo cid select-mode** command to restore the default.

By default, CIDs are cyclically selected in descending order.

In the dynamic mode, it is possible that multiple voice channels share one DLCI. The same CID at both ends may lead to a call collision. To prevent call collisions, you may configure different CID selection modes at both ends

Related command: **vofr**.

Example # Set the CID selection mode to min-poll on DLCI 100.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] fr dlci 100
[Sysname-fr-dlci-100] cid select-mode min-poll
```

display fr vofr-info

Syntax **display fr vofr-info** [**serial** *interface-number* [*dlci-number*]]

View Any view

Parameter **serial** *interface-number*: Displays the FRF.11 sub-channel information on a specified interface.

dlci-number: Virtual circuit number, in the range of 16 to 1007

Description Use the **display fr vofr-info** command to display the FRF.11 sub-channel information on a VoFR DLCI. You can use the **display fr vofr-info serial** *interface-number* command to display the FRF.11 sub-channel information on a specified interface sub-interface. The information of all FRF.11 sub-channels will be displayed if no interface sub-interface is specified. You can use the **display fr vofr-info** *dlci-number* to display the FRF.11 sub-channel information on a specified DLCI.

Example

```
<Sysname> display fr vofr-info
interface(dlci)       vofr-mode         cid     cid-type
Serial2/0:0(100)      vofr-nonstandard  5       frag-data
Serial2/0:0(100)      vofr-nonstandard  4       voice-signal
```

Table 700 Description on fields of the display fr vofr-info command

Field	Description
interface(dlci)	Frame relay interface name (DLCI number)
vofr-mode	VoFR call control protocol, for example, VoFR nonstandard-compatible and VoFR-Huawei-compatible.
cid	Voice channel number
cid-type	Type of a voice channel

entity vofr

Syntax **entity** *entity-number* **vofr**

undo entity *entity-number* **vofr**

View Voice dial program view

Parameter *entity-number*: Entity number, in the range of 1 to 2147483647.

vofr: VoFR entity

Description Use the **entity** command to enter VoFR entity view.

Use the **undo entity command to remove the existing voice entity.**

When you configure VoIP entities, POTS entities, and VoFR entities, they should be identified with different *entity-number*.

Example # Create a VoFR entity and number it 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 vofr
```

outband vofr

Syntax **outband vofr**

undo outband

View VoFR entity view

Parameter None

Description Use the **outband vofr** command to configure the out-of-band DTMF transmission mode.

Use the **undo outband** command to restore the default.

By default, the inband DTMF transmission mode is adopted.

Example # Configure the out-of-band DTMF transmission mode for VoFR entity 10.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 vofr
[Sysname-voice-dial-entity10] outband vofr
```

seq-number

Syntax **seq-number**

undo seq-number

View VoFR entity view

Parameter None

Description Use the **seq-number** command to configure the VoFR packets sent by the local voice gateway to carry a sequence number.

Use the **undo seq-number** command to restore the default.

By default, the VoFR packets sent by the local voice gateway do not carry any sequence number.

- *Usually, the configuration of the originating voice gateway determines whether VoFR packets carry a sequence number.*
- *Routers of some manufacturers do not comply with the above rule, but force VoFR packets to carry a sequence number when a specific codec is adopted. If a call failure or severe voice distortion occurs when the device is interconnected with a router of a third party, you can try making VoFR packets carry a sequence number.*
- *The terminating voice gateway can determine whether any voice packet loss, duplicate voice packet, or out-of-sequence occurs according to sequence numbers, which helps compensate voice. However, the use of sequence numbers will increase the required network bandwidth. Therefore, you can determine whether to use sequence numbers according to the actual condition.*

Example # Configure voice packets sent by VoFR entity 10 to carry a sequence number.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 vofr
[Sysname-voice-dial-entity10] seq-number
```

timestamp

Syntax **timestamp**

undo timestamp

View VoFR entity view

Parameter None

Description Use the **timestamp** command to configure VoFR packets sent by the local voice gateway to carry a timestamp.

Use the **undo timestamp** command to restore the default.

By default, the VoFR packets sent by the local voice gateway do not carry any timestamp.

Example # Configure voice packets sent by VoFR entity 10 to carry a timestamp.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] entity 10 vofr
[Sysname-voice-dial-entity10] timestamp
```

trunk-id

Syntax **trunk-id** *string*

undo trunk-id

View VoFR entity view

Parameter *string*: PSTN-dialed number, a string of 1 to 31 characters.

Description Use the **trunk-id** command to a PSTN-dialed number in the FRF.11 trunk mode.

Use the **undo trunk-id** command to restore the default.

By default, no PSTN-dialed number is configured in the FRF.11 trunk mode.

Related command: **call-mode**.

Example # Configure the PSTN-dialed number 3333 for VoFR entity 2222 in the FRF.11 trunk mode.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
```

```
[Sysname-voice-dial] entity 2222 vofr
[Sysname-voice-dial-entity2222] call-mode static
[Sysname-voice-dial-entity2222] trunk-id 3333
```

voice bandwidth

Syntax **voice bandwidth** *reserved-bps* [**reserved**]

undo voice bandwidth

View Frame relay class view

Parameter *reserved-bps*: Reserved voice bandwidth in bps, in the range of 8,000 to 45,000,000.

reserved: Reserves a VoFR voice bandwidth.

Description Use the **voice bandwidth** command to reserve a VoFR voice bandwidth.

Use the **undo voice bandwidth** command to remove the reserved bandwidth.

By default, no bandwidth is reserved for voice.

This command is configured in frame relay class view and takes effect only after the DLCI references such a frame relay class. Otherwise, no voice bandwidth will be available and call setup will fail.

Example # Reserve a maximum bandwidth of 8 kbps for voice in frame relay class test1 view

```
<Sysname> system-view
[Sysname] fr class test1
[Sysname-fr-class-test1] voice bandwidth 8000 reserved
```

vofr

Syntax **vofr** { **huawei-compatible** [**dce** | **dte**] | **motorola-compatible** [**dce** | **dte**] | **nonstandard-compatible signal-channel** *ccid-no* **data-channel** *dcid-no* [**keepalive**] }

undo vofr

View Interface DLCI view

Parameter **signal-channel** *ccid-no* **data-channel** *dcid-no*: FRF.11 sub-channel numbers respectively used by signaling and data when VoFR operates in the nonstandard-compatible mode, in the range of 4 to 255.

keepalive: Sends KeepAlive messages regularly. In the nonstandard-compatible mode, KeepAlive messages are regularly sent so as to monitor and control the

sub-channel status. If the **keepalive** keyword is configured, network congestion is considered occurring when one end fails to receive any KeepAlive message within a period of time. In this case, the active call control sub-channel will be deactivated, and no voice call can be set up any longer. If the **keepalive** keyword is not configured, the control sub-channel status is synchronized with the PVC status.

huawei-compatible: Adopts the Huawei-compatible mode.

motorola-compatible: Adopts the Motorola-compatible mode for compatibility with VoFR of Motorola routers.

nonstandard-compatible: Adopts the nonstandard-compatible mode for compatibility with VoFR of Cisco routers.

dce: Specifies the virtual circuit to serve as a DCE in compliance with Annex G.

dte: Specifies the virtual circuit to serve as a DTE in compliance with Annex G.

Description

Use the **vofr** command to configure a VoFR operation mode for a DLCI.

Use the **undo vofr** command to restore the default.

By default, no VoFR operation mode is configured.

If the VoFR operation mode is set to Motorola-compatible and the call mode is set to **static** (FRF.11 trunk mode), a call failure will occur.

In the Motorola-compatible mode, one DLCI can work in either the dynamic mode or the FRF.11 trunk mode. In the Huawei-compatible or Motorola-compatible mode, the T1.167 Annex G protocol is adopted. In this case, different ANNEX G-compliant control block types must be configured at both ends: one to DTE and the other to DCE.

Related command: **call-mode**.

Example

Set the call control protocol on DLCI 1000 to nonstandard-compatible, call control sub-channel number (ccid) to 4, and data sub-channel (dcid) to 5, and enable the regular sending of KeepAlive messages.

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] link-protocol fr ietf
[Sysname-Serial1/0] fr dlci 110
[Sysname-fr-dlci-Serial1/0-100] vofr nonstandard-compatible signal-c
hannel 4 data-channel 5 keepalive
```

Set the call control protocol on DLCI 200 to Huawei-compatible (DTE).

```
<Sysname> system-view
[Sysname] interface serial 1/0
[Sysname-Serial1/0] link-protocol fr ietf
[Sysname-Serial1/0] fr dlci 200
[Sysname-fr-dlci-Serial1/0-100] vofr huawei-compatible dte
```

vofr frf11-timer

Syntax **vofr frf11-timer** *time*

undo vofr frf11-timer

View Voice view

Parameter *time*: Trunk Wait timer length in the FRF.11 trunk mode in seconds, in the range of 10 to 600.

Description Use the **vofr frf11-timer** command to configure the trunk wait timer length in the FRF.11 trunk mode.

Use the **undo vofr frf11-timer** command to restore the default.

By default, the trunk wait timer length is 30 seconds.

This command has global significance. The configuration is valid for all FRF.11 trunk calls after the command is executed.

- *The Trunk Wait timer is specific to the FRF.11 trunk mode. Within the trunk wait timer length, incoming calls are prohibited and received voice packets are dropped.*
- *No signaling is exchanged in the FRF.11 trunk mode. When one voice gateway receives the first voice packet from its peer voice gateway over a dedicated voice channel, the former considers that a call is coming. When either party involved in a call hangs up, the peer voice gateway (relative to the party who hangs up) will still keep sending voice packets to the local voice gateway. Without the Trunk Wait timer mechanism, the local voice gateway will immediately alert the party who has hung up so that this party could never hang up successfully in the FRF.11 trunk mode.*

Related command: **call-mode**.

Example # Configure the Trunk Wait timer length in the FRF.11 trunk mode to 40 seconds.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] vofr frf11-timer 40
```

180 VOICE RADIUS CONFIGURATION COMMANDS

aaa-client

Syntax **aaa-client**

View Voice view

Parameter None

Description Use the **aaa-client** command to enter voice AAA client view.

Example # Enter voice AAA client view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa]
```

accounting

Syntax **accounting**

undo accounting

View Access number view

Parameter None

Description Use the **accounting** command to enable the RADIUS accounting function for users who dial some access number.

Use the **undo accounting** command to disable the RADIUS accounting function.

By default, the RADIUS accounting function is disabled for users who dial access numbers.

On one voice gateway, the RADIUS accounting function for one-stage dialing users (who dial a called number to originate a call after picking up the phone) differs from that for two-stage dialing users (who first dial an access number and then a called number to originate a call after picking up the phone). This command is only applicable to an access number, namely, two-stage dialing users.

With the RADIUS accounting function enabled, the RADIUS server will perform accounting for all users who use this access number. With the function disabled, the RADIUS server will not perform accounting for users who dial the access number.

Related command: **gw-access-number**, **acct-method**, and **accounting-did**.

Example # Enable the RADIUS accounting function for users who dial the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] accounting
```

Disable the RADIUS accounting function for users who dial the access number 17909.

```
[Sysname-voice-dial-anum17909] undo accounting
```

accounting-did

Syntax **accounting-did**

undo accounting-did

View Voice AAA client view

Parameter None

Description Use the **accounting-did** command to enable the RADIUS accounting function for all one-stage dialing users.

Use the **undo accounting-did** command to disable the RADIUS accounting function.

By default, the RADIUS accounting function is disabled for all one-stage dialing users.

On one voice gateway, the RADIUS accounting for one-stage dialing users is separated from that for two-stage dialing users. This command is applicable to only one-stage dialing users. With this function enabled, the RADIUS server will perform RADIUS accounting for all calls originated by one-stage dialing users. With this function disabled, the RADIUS server will not perform accounting for any calls originated by one-stage dialing users.

Related command: **acct-method** and **accounting**.

Example # Enable the accounting function for all one-stage dialing users.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa] accounting-did
```

Disable the accounting function for all one-stage dialing users.

```
[Sysname-voice-aaa] undo accounting-did
```

acct-method

Syntax **acct-method** { **start-ack** | **start-no-ack** | **stop-only** }

undo acct-method

View Voice AAA client view

Parameter **start-ack**: The voice gateway sends an Accounting_Start request to the RADIUS server and needs to receive an Accounting_Start acknowledgment before connecting a call. The voice gateway sends an Accounting_Stop request to the RADIUS server but does not need to receive an Accounting_Stop acknowledgment before releasing the call.

start-no-ack: The voice gateway sends an Accounting_Start request or Accounting_Stop request to the RADIUS server before connecting or releasing a call, and directly connects or releases the call without waiting for an acknowledgment from the RADIUS server.

stop-only: The voice gateway sends an Accounting_Stop request to the RADIUS server before releasing a call, and directly releases the call without waiting for an acknowledgment from the RADIUS server.

Description Use the **acct-method** command to configure an accounting method for the RADIUS client.

Use the **undo acct-method** command to restore the default.

By default, the accounting method is **start-no-ack**.

Related command: **accounting** and **accounting-did**.

Example # Set the accounting method to **start-ack**.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa] acct-method start-ack
```

Restore the default accounting method.

```
[Sysname-voice-aaa] undo acct-method
```

authentication

Syntax **authentication**

undo authentication

View Access number view

Parameter None

Description Use the **authentication** command to enable the RADIUS authentication function for users who dial some access number.

Use the **undo authentication** command to disable the RADIUS authentication function.

By default, the RADIUS authentication function is disabled for users who dial access numbers.

For each access number, you can specify the RADIUS server to perform authentication for users who dial it. If the authentication function is enabled for users who dial some access number, only users who pass authentication can be authorized to make IP calls. If the authentication function is disabled, users who dial the access number can directly make IP calls no matter whether they are legal.

The authentication function must be enabled before the authorization function. When the authentication function is disabled, the authorization function will automatically be disabled, and meanwhile, the **authorization** and **undo authorization** commands will be unavailable.

Related command: **gw-access-number** and **authorization**.

Example # Enable the authentication function for users who dial the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] authentication
```

Disable the authentication function for users who dial the access number 17909.

```
[Sysname-voice-dial-anum17909] undo authentication
```

authentication-did

Syntax **authentication-did**

undo authentication-did

View Voice AAA client view

Parameter None

Description Use the **authentication-did** command to enable the authentication function for all one-stage dialing users.

Use the **undo authentication-did** command to disable the authentication function.

By default, the authentication function is disabled for all one-stage dialing users.

This command is applicable to only one-stage dialing users, instead of two-stage dialing users.

With this function enabled, the calling number of one-stage dialing users who want to make IP calls is sent to the RADIUS server for authentication. Only users who pass authentication can make IP calls. Those who fail authentication will be disconnected and cannot make IP calls.

The authentication function must be enabled before the authorization function. When the authentication function is disabled, the authorization function will automatically be disabled, and meanwhile, the **authorization-did** and **undo authorization-did** commands will be unavailable.

Related command: **authorization-did**.

Example # Enable the authentication function for one-stage dialing users.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa] authentication-did
```

authorization

Syntax **authorization**

undo authorization

View Access number view

Parameter None

Description Use the **authorization** command to enable the authorization function for users who dial some access number.

Use the **undo authorization** command to disable the authorization function.

By default, the authorization function is disabled for users who dial access numbers.

With this function enabled, called numbers will be sent to the RADIUS server for authorization after users who dial some access number to make IP calls pass authentication.

You must enable the authentication function (by using the **authentication** command) before the authorization function. Otherwise, the **authorization** command is unavailable.

Related command: **gw-access-number** and **authentication**.

Example # Enable the authorization function for users who dial the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] authentication
[Sysname-voice-dial-anum17909] authorization
```

Disable the authorization function for users who dial the access number 17909.

```
[Sysname-voice-dial-anum17909] undo authorization
```

authorization-did

Syntax **authorization-did**

undo authorization-did

View Voice AAA client view

Parameter None

Description Use the **authorization-did** command to enable the authentication function for all one-stage dialing users.

Use the **undo authorization-did** command to disable the authorization function for all one-stage dialing users.

By default, the authorization function is disabled for all one-stage dialing users.

This command is applicable to only one-stage dialing users, instead of two-stage dialing users. With this function enabled, called numbers will be sent to the RADIUS server for authorization after users who dial some access number to make IP calls pass authentication.

You must enable the authentication function before the authorization function. Otherwise, the **authorization-did** command is unavailable.

Related command: **authentication-did**.

Example # Enable the authorization function for one-stage dialing users.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa] authentication-did
[Sysname-voice-aaa] authorization-did
```

Disable the authorization function for one-stage dialing users.

```
[Sysname-voice-aaa] undo authorization-did
```

callednumber receive-method

Syntax **callednumber receive-method** { **immediate** | **terminator** }

undo callednumber receive-method

View Access number view

Parameter **immediate**: Specifies the voice gateway to originate a call immediately it collects all digits of a called number.

terminator: Specifies users to press the dial terminator # after dialing a called number.

Description Use the **callednumber receive-method** command to configure the method of collecting digits of a called number.

Use the **undo callednumber receive-method** command to restore the default.

By default, users need to press the dial terminator # after dialing all digits of a called number.

This command is applicable to both the one-stage dialing process and two-stage dialing process. In the **terminator** mode, the voice gateway can immediately originate a call only after users dial a called number and press the dial terminator #, and otherwise, the voice gateway will not originate a call until timeout. In the **immediate** mode, the voice gateway can originate a call immediately it collects all digits of a called number, without waiting users to press the dial terminator #. The **immediate** mode simplifies users' operations.

Related command: **gw-access-number**.

Example # Set the method of collecting digits of called numbers to **immediate** for the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] callednumber receive-method immediate
```

Restore the default method of collecting digits of called numbers for the access number 17909.

```
[Sysname-voice-dial-anum17909] undo callednumber receive-method
```

card-digit

Syntax **card-digit** *card-digit*

undo card-digit

View Access number view

Parameter *card-digit*: Number of digits in a card number, in the range of 1 to 31.

Description Use the **card-digit** command to configure the number of digits in a card number for some access number in the card number/password process.

Use the **undo card-digit** command to restore the default.

By default, the number of digits in a card number is 12 only when an access number is already configured for the card number/password process (by using the **process-config** command).

Note that:

- This command is used to configure the number of digits in a card number for the card number/password process. Once the number of digits is fixed, all users who use the access number must enter a fixed-length card number. Otherwise, the voice gateway will report an error.
- The **card-digit** command is available in access number view only after you use the **process-config** command to specify the dialing process as card number/password process.

Related command: **gw-access-number** and **process-config**.

Example # Specify the number of digits in a card number as 10 for the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] process-config cardnumber
[Sysname-voice-dial-anum17909] card-digit 10
```

cdr

Syntax **cdr** { **buffer** *size-number* | **duration** *time-length* | **threshold** *percentage* }

undo cdr { **all** | **buffer** | **duration** | **threshold** }

View Voice AAA client view

Parameter **buffer** *size-number*: Specifies the number of CDRs that can be saved in the buffer. The *size-number* argument ranges from 0 to 500, with a default of 50. The value "0" indicates that no CDR can be saved.

duration *time-length*: Specifies the lifetime of CDRs in seconds. The *time-length* argument ranges from 0 to 2,147,483,647, with a default of 86,400. The value "0" indicates that no CDR can be saved.

threshold *percentage*: Specifies the alarm threshold in percents for CDRs. When the percentage of the saved CDRs in the total CDRs that can be saved in the buffer reaches the alarm threshold, the voice gateway will generate alarm information once. The *percentage* argument ranges from 0 to 100, with a default of 80. The value "0" indicates that no alarm information will be output.

Description Use the **cdr** command to configure a rule for saving CDRs.

Use the **undo cdr** command to restore the default saving rule, and the **undo cdr all** command to restore the values of **buffer**, **duration**, and **threshold** all to the defaults.

The voice gateway will save a certain amount of CDRs according to the configured rule. When you set the number of CDRs that can be saved or the lifetime of CDRs, the voice gateway will judge whether the existing CDRs will be deleted. If so, the voice gateway will prompt for confirmation and determine whether to validate the configuration according to your confirmation.

If both the **buffer** and **duration** keywords are specified, the number of saved CDRs cannot exceed the limit set by the **buffer** keyword. If large traffic is generated in a period of time, the CDRs for the calls completed earliest will be removed to keep the number of saved CDRs under the limit even if they have not reached the lifetime.

Related command: **display voice call-history-record**.

Example # Set the number of CDRs that can be saved to 400.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] aaa-client
[Sysname-voice-aaa] cdr buffer 400
```

Set the lifetime of CDRs to 10 hours.

```
[Sysname-voice-aaa] cdr duration 36000
```

Set the alarm threshold for CDRs to 10%.

```
[Sysname-voice-aaa] cdr threshold 10
```

display voice access-number

Syntax **display voice access-number**

View Any view

Parameter None

Description Use the **display voice access-number** command to display the configuration information and access numbers in voice AAA client view.

The information displayed includes:

- Accounting method
- Enabling or disabling of the authentication, authorization, and accounting functions for one-stage dialing users
- Rule for saving CDRs
- Configuration information for all access numbers

Related command: **gw-access-number** and **aaa-client**.

Example # Display the configuration information and access numbers.

```
<Sysname> display voice access-number
AAA configuration :
accounting-method               =   start-ack
    accounting-did                      =   on
    authentication-did              =   off
    authorization-did               =   on
    call history rule:
       cdr buffer                       =   100
       cdr duration             =   86400
       cdr threshold            =   50

access number: [ 17909 ]
dialing process         =   cardnumber
        accounting                      =   on
        authentication              =   on
        authorization               =   on
        callednum receive       =   termintor
        card digit                      =   12
        password digit          =   6
        redialing times         =   2

access number: [ 201 ]
dialing process         =   voice-caller
        accounting                      =   off
        authentication              =   off
        authorization               =   off
        callednum receive       =   immediate
redialing times         =   2
        language selected     =   Chinese
```

Table 701 Description on fields of the display voice access-number command

Field	Description
accounting-method	Accounting method, including start-ack, start-no-ack, and stop-only. See "acct-method" on page 2723.
accounting-did	Accounting function for one-stage dialing users ■ on: Enabled ■ off: Disabled See "authentication-did" on page 2724.
authentication-did	Authentication function for one-stage dialing users ■ on: Enabled ■ off: Disabled See "authentication-did" on page 2724.
authorization-did	Authorization function for one-stage dialing users on: Enabled off: Disabled See "authentication-did" on page 2724.
call history rule	Rule for saving CDRs
cdr buffer	Number of CDRs that can be saved. See "cdr" on page 2728.
cdr duration	Lifetime of CDRs. See the **cdr duration** command.
cdr threshold	CDR alarm threshold. See "cdr" on page 2728.
access number	Access number, for example, 17909. See"gw-access-number" on page 2736.
dialing process	Two-stage dialing process, including card number/password process, caller number process, caller number process with IVR. See "process-config" on page 2738.
accounting	Accounting function for two-stage dialing users ■ on: Enabled ■ off: Disabled See "accounting" on page 2721.
authentication	Authentication function for two-stage dialing users ■ on: Enabled ■ off: Disabled See "authentication" on page 2724
authorization	Authorization function for two-stage dialing users ■ on: Enabled ■ off: Disabled See "authentication" on page 2724.
callednum receive	Method of collecting digits of a called number, including terminator and immediate. See "callednumber receive-method" on page 2727.
card digit	Number of digits in a card number, displayed only in the card number/password process. See "card-digit" on page 2728.

Table 701 Description on fields of the display voice access-number command

Field	Description
password digit	Number of digits in a password, displayed only in the card number/password process. See "password-digit" on page 2737.
redialing times	Number of redial attempts, displayed in the card number/password process or caller number process with IVR. See "redialtimes" on page 2740.
language selected	Language selection function, Chinese and English available, displayed only in the caller number process with IVR. See "selectlanguage" on page 2741.

display voice call-history-record

Syntax **display voice call-history-record** { **all** | **callednumber** *called-number* | **callingnumber** *calling-number* | **cardnumber** *card-number* | **last** *last-number* | **line** *line-number* | **remote-ip-addr** *ip-address* }

View Any view

Parameter **all**: Displays all call records.

callednumber *called-number*: Displays call records by called number. The *called-number* argument is a string of up to 31 characters, consisting of digits 0 through 9 and the asterisk *.

callingnumber *calling-number*: Displays call records by calling number. The *calling-number* argument is a string of up to 31 characters, consisting of digits 0 through 9 and the asterisk *.

card *card-number*: Displays call records by prepaid card number. The *card-number* argument is a string of up to 31 characters.

last *last-number*: Displays the specified number of latest call records. The *last-number* argument ranges from 1 to 500.

line *line-number*: Displays incoming or outgoing call records by voice subscriber line of the voice gateway. The value range of the *line-number* argument varies with devices.

remote-ip-addr *ip-address*: Displays call records by callee's IP address. The *ip-address* argument represents a callee's IP address.

Description Use the **display voice call-history-record** command to display voice RADIUS call records.

If the *ip-address* argument is specified, the system displays call records by callee's IP address. If the *last-number* argument is specified, the voice gateway displays the specified number of latest call records, and if a value greater than the number of actual call records is specified, the voice gateway will display all call records.

The system finds call records by the search condition. If the voice gateway fails to find a call record or the found record is null, the voice gateway will give prompt information.

Related command: **cdr**.

Example # Display call records by calling number.

```
<Sysname> display voice call-history-record callingnumber 4000
  Call records of voice RADIUS:
  #
  CallRecord [ 0 ]:
    CallReference    = 46
    CallRecordTime   = Oct 20, 2006 16:45:47
    CardNumber       = None
    AccessNumber     = None

    Incoming call leg:
      CallingNumber  = 4000
      SignalType     = FXS/O
      VoiceInterface = 1/0
      SetupTime      = Oct 20, 2006 16:45:43
      ConnectTime    = Oct 20, 2006 16:45:45
      ReleaseTime    = Oct 20, 2006 16:45:47
      SendPackets    = 71 packages
      SendBytes      = 2982 bytes
      ReceivePackets = 111 packages
      ReceiveBytes   = 4662 bytes

    Outgoing call leg [ 0 ]:
      CalledNumber   = 2000
      CallDuration   = 00h 00m 02s
      EncodeType     = G729R8
      DecodeType     = G729R8
      ReleaseCause   = Called hook on
      SignalType     = SIP
      IpAddress/Port = 1.1.1.19/5060
      SetupTime      = Oct 20, 2006 16:45:43
      ConnectTime    = Oct 20, 2006 16:45:45
      ReleaseTime    = Oct 20, 2006 16:45:47
      SendPackets    = 111 packages
      SendBytes      = 4662 bytes
      ReceivePackets = 72 packages
      ReceiveBytes   = 3024 bytes
  #
  The end
```

Table 702 Description on fields of the display voice call-history-record command

Field	Description
Call records of voice RADIUS	Voice RADIUS call records
CallRecord [0]	Call record number
CallReference	Voice RADIUS module call identification
CallRecordTime	Time when a call is recorded
CardNumber	Card number
AccessNumber	Access number

Table 702 Description on fields of the display voice call-history-record command

Field	Description
Incoming Call Leg	Information of the incoming call leg
CallingNumber	Calling number
SignalType	Signaling protocol (for example, R2, E&M, H.323)
VoiceInterface	Voice interface
SetupTime	Call setup time
ConnectTime	Call-connected time
ReleaseTime	Call release time
SendPackets	Packets sent
SendBytes	Bytes sent
ReceivePackets	Packets received
ReceiveBytes	Bytes received
Outgoing call leg [0]	Information of the outgoing call leg. One call may involves multiple outgoing call legs. [0] identifies one outgoing call leg.
CalledNumber	Called number
CallDuration	Call duration
EncodeType	Encoding type
DecodeType	Decoding type
ReleaseCause	Call release cause
SignalType	Signaling protocol (for example, R2, E&M, and H.323) on the terminating side
VoiceInterface	Voice interface
IpAddress/Port	IP address and port number
SetupTime	Call setup time
ConnectTime	Call-connected time
ReleaseTime	Call release time
SendPackets	Packets sent
SendBytes	Bytes sent
ReceivePackets	Packets received
ReceiveBytes	Bytes received

display voice radius statistic

Syntax **display voice radius statistic**

View Any view

Parameter None

Description Use the **display voice radius statistic** command to display statistics of messages exchanged between the voice RADIUS module, call management center (CMC) module, and AAA module.

Related command: **reset voice radius statistic**.

Example # Display statistics of messages exchanged between the voice RADIUS module, CMC module, and AAA module.

```
<Sysname> display voice radius statistic
VORDS => AAA:
        Authen_Request                      =  0
        Author_Request                      =  0
        AcctReq_PstnCaller              =  0
        AcctReq_VoipCaller              =  0
        AcctReq_PstnCalled              =  0
        AcctReq_VoipCalled              =  0
        Account_Stop                            =  0
        Leaving                                 =  0
   AAA => VORDS:
        Authen_Accept                           =  0
        Authen_Reject               =  0
        Author_Accept               =  0
        Author_Reject               =  0
        AcctRsp_PstnCaller          =  0
        AcctRsp_VoipCaller          =  0
        AcctRsp_PstnCalled          =  0
        AcctRsp_VoipCalled          =  0
        Account_Ok                    =  0
        Account_Failure             =  0
        Cut                             =  0
   CMC => VORDS:
        Setup                         =  0
        Alerting                    =  0
        Connect                     =  0
        Release                     =  0
        DtmfInformation                     =  0
        ChannelReady                =  0
        FaxVoiceSwitch              =  0
        FaxTone                      =  0
```

Table 703 Description on fields of the display voice radius statistic command

Field	Description
VORDS=>AAA:	Messages from the voice RADIUS module to the AAA module
Authen_Request	Authentication_Request message
Author_Request	Authorization_Request message
AcctReq_PstnCaller	Accounting_Request message for PSTN caller
AcctReq_VoipCaller	Accounting_Request message for VoIP caller
AcctReq_PstnCalled	Accounting_Request message for PSTN callee
AcctReq_VoipCalled	Accounting_Request message for VoIP callee
Account_Stop	Accounting_Stop message
Leaving	Leaving message
AAA=>VORDS	Messages from the AAA module to the voice RADIUS module
Authen_Accept	Authentication_Accept message
Authen_Reject	Authentication_Reject message
Author_Accept	Authorization_Accept message
Author_Reject	Authorization_Reject message

Table 703 Description on fields of the display voice radius statistic command

Field	Description
AcctRsp_PstnCaller	Accounting_Response message for PSTN caller
AcctRsp_VoipCaller	Accounting_Response message for VoIP caller
AcctRsp_PstnCalled	Accounting_Response message for PSTN callee
AcctRsp_VoipCalled	Accounting_Response message for VoIP callee
Account_Ok	Accounting_Ok message
Account_Failure	Accounting_Failure message
Cut	Cut message
CMC=>VORDS	Messages from the CMC module to the voice RADIUS module
Setup	Setup message
Alerting	Alerting message
Connect	Connect message
Release	Release message
DtmfInformation	DTMF digit
ChannelReady	Channel_Ready message
FaxVoiceSwitch	Fax_Voice_Switch message
FaxTone	Fax_Tone message

gw-access-number

Syntax **gw-access-number** *access-number*

undo gw-access-number { *access-number* | **all** }

View Voice dial program view

Parameter *access-number*: Access number (for example, 169 and 17909), a string of up to 31 characters consisting of digits 0 through 9 and the wildcard ".". The wildcard "." represents a digital character and must follow a digit or appear separately.

all: Deletes all access numbers.

Description Use the **gw-access-number** command to configure an access number or enter access number view.

Use the **undo gw-access-number** command to delete one or all access numbers.

By default, no access number is configured.

When you delete all configured access numbers, the voice gateway will give alarm information, requiring you to make a confirmation. You can press <Y> to delete all access numbers or press <N> to cancel the operation.

An access number can contain up to 31 characters, but no unacceptable characters such as a letter. At most 100 access numbers can be configured for the voice gateway.

The shortest match and exact match are preferred for access number match. If an access number template is the same as some voice entity template, the global number substitution rules in voice dial program view and those in voice subscriber line view will be valid for the access number, but no entity substitution rule can be matched in access number view.

Example # Add the access number 17909 and enter access number view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909]
```

Add the access number 179 and enter access number view.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 179..
[Sysname-voice-dial-anum179..]
```

Delete the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] undo gw-access-number 17909
```

Delete all access numbers.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] undo gw-access-number all
Delete all access numbers, are you sure? (Y/N) y
```

password-digit

Syntax **password-digit** *password-digit*

undo password-digit

View Access number view

Parameter *password-digit*: Number of digits in a password, in the range of 1 to 16.

Description Use the **password-digit** command to configure the number of digits in a password for some access number in the card number/password process.

Use the **undo password-digit** command to restore the default number of digits in a password for some access number in the card number/password process.

This command is unavailable for the caller number process with IVR. By default, the number of digits in a password for some access number in the card number/password process is 6.

Before executing the **password-digit** command, you must use the **process-config** command to specify the two-stage dialing process for the configured access number as card number/password process. The **password-digit** command is available only in access number view.

Related command: **gw-access-number** and **process-config**.

Example # Specify the number of digits in a password as 4 for the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] process-config cardnumber
[Sysname-voice-dial-anum17909] password-digit 4
```

Restore the default number of digits in a password for the access number 17909.

```
[Sysname-voice-dial-anum17909] undo password-digit
```

process-config

Syntax **process-config** { **callernumber** | **cardnumber** | **voice-caller** }

undo process-config

View Access number view

Parameter **callernumber**: Specifies the two stage-dialing process as caller number process. After a user dials an access number, the voice gateway will continue to play dial tones, prompting for a called number. In this process, the user authentication is implemented by identifying the calling number, and no more additional parameter configurations are required.

cardnumber: Specifies the two-stage dialing process as card number/password process. After a user dials an access number, the voice gateway will continue to play prompt tones, requiring the user to enter a card number and password. In this process, the user authentication is implemented by identifying the prepaid card number and password, and you can configure parameters by using the **card-digit**, **password-digit**, and **redialtimes** commands.

voice-caller: Specifies the two-stage dialing process as caller number process with IVR. After a user dials an access number, the voice gateway will play prompt tones, requiring the user to dial a called number. In this process, the user authentication

is implemented by identifying the calling number. If the authentication succeeds, the voice gateway plays prompt tones, requiring the user to dial a called number. In addition, you can configure the number of redial attempts by using the **redialtimes** command, and the language in which the prompt tones are played by using the **selectlanguage** command.

Description

Use the **process-config** command to specify a dialing process for an access number.

Use the **undo process-config** command to restore the default dialing process for an access number.

By default, the caller number process with IVR is specified for all access numbers.

Each access number has a specific dialing process. Calls originated by users who dial a certain access number are established in accordance with the same dialing process.

Differences between the caller number process and the caller number process with IVR are as follows:

- In the caller number process, after a user dials an access number, the voice gateway plays only dial tones (long tones).
- In the caller number process with IVR, after a user dials an access number, the voice gateway will play prompt tones, requiring the user to dial a called number.

In the card number/password process, with the authentication function disabled, a user can enter any two numbers as a card number and password respectively to make an IP call as long as they meet the length requirements.

After a dialing process is specified, parameters not related to the process are set to the default values and the corresponding commands are unavailable. Parameters related to the card number/password process include number of digits in a card number and number of digits in a password. The language selection function is applicable only to the caller number process with IVR, while the number of redial attempts is applicable to only the card number/password process and the caller number process with IVR.

Related command: **gw-access-number**, **card-digit**, **password-digit** and **selectlanguage**.

Example

Specify the dialing process for the access number 17909 as card number/password process.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] process-config cardnumber
```

Restore the default dialing process for the access number 17909.

```
[Sysname-voice-dial-anum17909] undo process-config
```

redialtimes

Syntax **redialtimes** *redialtimes-number*

undo redialtimes

View Access number view

Parameter *redialtimes-number*: Number of redial attempts, in the range of 0 to 10. In the card number/password process, this argument may refer to the times of reselecting a language or redialing a card number, password, or a called number. In the caller number process with IVR, this argument may refer to the times of reselecting a language or redialing a called number.

Description Use the **redialtimes** command to configure the number of redial attempts in each dialing step for an access number.

Use the **undo redialtimes** command to restore the default number of redial attempts for an access number.

By default, the number of redial attempts in each dialing step is 2 for an access number.

The *redialtimes-number* argument refers to the number of redial attempts, that is, the number of dial attempts is the number of redial attempts plus 1.

This command is unavailable in the caller number process

For the card number/password process, you can use the **redialtimes** command to set times of reselecting a language and times of redialing a card number, password, or called number. To make an IP call, a user first dials an access number, then selects a language, next enters a prepaid card number and password, and finally dials a called number. Any error in each dialing step may lead to a dialing failure.

For the caller number process with IVR, you can use the **redialtimes** command to set times of reselecting a language and times of redialing a called number.

Related command: **gw-access-number** and **process-config**.

Example # Set the number of redial attempts to 4 for the access number 17909.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] process-config cardnumber
[Sysname-voice-dial-anum17909] redialtimes 4
```

reset voice radius statistic

Syntax **reset voice radius statistic**

View User view

Parameter None

Description Use the **reset voice radius statistic** command to clear statistics of messages exchanged between the voice RADIUS module, CMC module, and AAA module.

Related command: **display voice radius statistic**.

Example # Clear the statistics of messages exchanged between the voice RADIUS module, CMC module, and AAA module.

```
<Sysname> reset voice radius statistic
```

selectlanguage

Syntax **selectlanguage** { **enable** | **chinese** | **english** }

undo selectlanguage

View Access number view

Parameter **enable**: Enables the language selection function so that users can select a language to play prompt tones.

chinese: Plays prompt tones in Chinese.

english: Plays prompt tones in English.

Description Use the **selectlanguage** command to configure a language in which prompt tones are played in the caller number process with IVR.

Use the **undo selectlanguage** command to restore the default.

By default, prompt tones are played in Chinese.

This command is available only in the caller number process with IVR.

Related command: **gw-access-number** and **process-config**.

Example # Configure the voice gateway to play prompt tones in English.

```
<Sysname> system-view
[Sysname] voice-setup
[Sysname-voice] dial-program
```

```
[Sysname-voice-dial] gw-access-number 17909
[Sysname-voice-dial-anum17909] process-config voice-caller
[Sysname-voice-dial-anum17909] selectlanguage english
```